LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Lahden ammattikorkeakoulun verkkotekniikan laboratorion etä-käyttöjärjestelmän laajennus

NDG Netlab -laajennus

LAHDEN AMMATTIKORKEAKOULU
Insinööri AMK, Tieto- ja viestintätekniikka
Kevät 2018
Ville Heinonen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Heinonen, Ville	Opinnäytetyö, AMK	Kevät 2018
	Sivumäärä	
	38	

Työn nimi

LAMK:n verkkotekniikan laboratorion etäkäyttöjärjestelmän laajennus
NDG Netlab -laajennus

Tutkinto

Insinööri AMK, Tieto- ja viestintätekniikka

Tiivistelmä

Opinnäytetyön tavoite oli laajentaa Lahden ammattikorkeakoulun verkkotekniikan laboratorion etäkäyttöjärjestelmää uusilla laitesoluilla. Tämä kattoi laajennusvaihtoehtojen vertailun ja valitun ratkaisun asennuksen, joka sisälsi kolme laitesolua.

Laajennusvaihtoehdot olivat AE monikäyttöinen laitesolu ja AE monikäyttöinen laitesolu Ciscon Adaptive Security Appliancella. Vaihtoehdoista valittiin standardisolu ilman ASA-laitetta, sen suoraviivaisemman asennuksen takia.

Valittu laitesolu muodostuu kolmesta kytkimestä ja kolmesta reitittimestä, jotka muodostavat lähiverkon. Tämän verkon arkkitehtuuri pohjaa OSI-malliin ja operoi IP-, UDP-, SNMP- ja TFTP-verkkoprotokollien avulla.

Laitesolu on sijoitettu palvelimen taakse, mikä erottaa sen julkisesta verkosta. Tiedonsiirto tapahtuu yhteyspalvelimen välityksellä, mihin käyttäjä ottaa yhteyden etänä verkkokäyttöliittymän kautta. Tämä NETLAB+-käyttöliittymä mahdollistaa harjoitusten tekemisen laitteilla, minkä lisäksi se avustaa kokonaisuuden hallinnassa ja ylläpidossa.

Fyysisen asennuksen ja konfiguroinnin jälkeen saatiin käyttöön kolme uutta laitesolua. Nämä solut tehostivat toimeksiantajan järjestelmän toimintaa toivotulla tavalla ja täyttivät työn tavoitteen. Tämä kuitenkin saavutti standardisolujen ylärajan, minkä vuoksi jatkossa lisäykset eivät voi pohjata niihin.

Tulevaisuudessa kyseisen järjestelmän laajennukset täytyy tehdä joko ASA-laitesoluilla, hyvin rajallisilla uniikeilla soluilla tai versiota vaihtamalla.

Asiasanat

Lähiverkko, Etäkäyttö, Netlab

Abstract

Author(s)	Type of publication	Published
Heinonen, Ville	Bachelor's thesis	Spring 2018
	Number of pages	
	38	

Title of publication

Extension of LAMK's networking laboratory's remote access system
NDG Netlab extension

Name of Degree

Bachelor of Engineering, Information technology

Abstract

The objective of this thesis was to extend the remote access system the networking laboratory of Lahti University of Applied Sciences. This included comparison between two extension possibilities and the installation itself.

The comparison was between AE Multi-Purpose Academy Pod with and without Cisco Adaptive Security Appliance. The option without the Adaptive Security Appliance was chosen, due to its more streamlined installation.

The chosen pod is comprised of three switches and three routers. These devices form an OSI model based local area network, which is operated by IP, UDP, SNMP, and TFTP protocols.

This pod is placed behind a server, which excludes the pod from the internet. Operations with the devices are therefore intermediated by the server. The server is in turn accessed through a network interface. The interface in this case is NETLAB+, which enables users to do exercises with the devices and helps with management as well as administration.

The installation resulted in three new equipment pods. These pods improved the efficiency of school's system and therefore fulfilled the objective of the thesis. However, this process reached the maximum of standard pods in a system.

In conclusion, the future installations must be made with Adaptive Security Appliance pods or with limited custom pods unless the system itself is upgraded.

Keywords

local area networks, remote access, Netlab

SISÄLLYS

1 JOHDANTO

Lahden ammattikorkeakoulu (LAMK) on monimuotoista koulutusta tarjoava korkeakoulu, jonka koulutusalat kattavat liiketalouden ja matkailun, muotoilun ja viestinnän, sosiaali- ja terveysalan sekä tekniikan. Tämän LUT-konsernin tytäryhtiön tavoite on kouluttaa asiantuntijoita edellä mainituille aloille ja vahvistaa alueen yleistä osaamista näillä kentillä. (LAMK 2018.)

Lahden ammattikorkeakoulun verkkotekniikan laboratorio on tekniikan alan tietoliikennetekniikan suuntautumisvaihtoehdon opetuspiste, missä valtaosa opetuksesta ja materiaalista sijaitsee. Esimerkkinä tästä toimii työssä laajennetun NDG NETLAB+:n paikallinen laitteisto, joka on sijoitettu laboratorion tiloihin. Verkkotekniikan laboratorio oli myös virallinen toimeksiantaja tällä tutkimustyölle.

Tavoitteena oli tarkastella kahta NDG NETLAB+-ympäristön etäkäyttöjärjestelmän laajennusvaihtoehtoa ja toteuttaa tilanteeseen sopivammaksi valikoitunut ratkaisu. Tällä pyrittiin tehostamaan laitteiston käytettävyyttä ja samalla helpottamaan sen siirtoa tulevaan tekniikan alan toimipisteeseen syyskuussa 2018. Työn aikana vertailtiin toteutuksien eroja sekä niiden laitteisto- ja tilarajoituksia, minkä jälkeen suoritettiin fyysinen asennus.

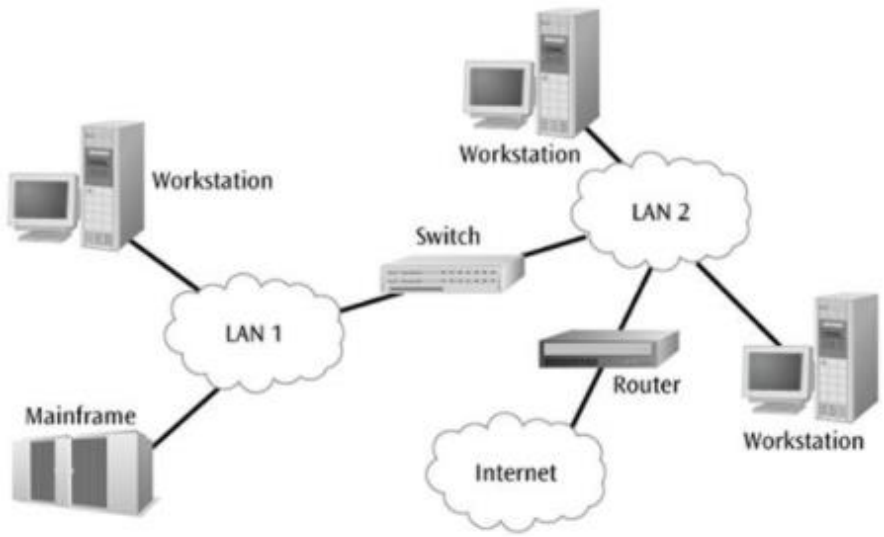
Tässä opinnäytetyössä käydään aluksi läpi lähiverkon toimintaa ja elementtejä, mistä siirrytään tarkastelemaan etäkäyttöä. Tämän jälkeen tutustutaan itse NETLAB+-järjestelmään. Työn viimeisessä luvussa syvennytään itse laajennukseen ja aiemmassa luvussa listattuihin tutkimuksen tavoitteisiin.

2 LÄHIVERKKO

2.1 Tietoliikenteen lähiverkko

Lähiverkko (Local Area Network) on paikallinen tietoliikenneverkko, joka liittää rajatun alueen sisällä olevat tietokoneet ja oheislaitteet toisiinsa. Tämä asennus pyrkii luomaan nopean ja tehokkaan yhteyden laitteiden välille, minkä lisäksi sen läpi voidaan tarjota useita erilaisia toimintoja. (White 2011, 196 - 197.)

Kaikki datan välitykseen perustuvat sovellukset ovat ainakin osaksi lähiverkon vastuulla, mistä johtuen tämän osa-alueen tehtävät ovat erittäin riippuvaisia toimintaympäristöstä. Esimerkiksi on hyvin tavanomaista, että lähiverkko toimii välipintana, joka yhdistää laitteet laajaverkkoon ja sitä myöten internetiin kuten kuviossa 1. (White 2011, 197.)



Kuvio 1. Lähiverkko, joka yhdistää toisen lähiverkon, internetin ja keskustietokoneen (White 2011, 198)

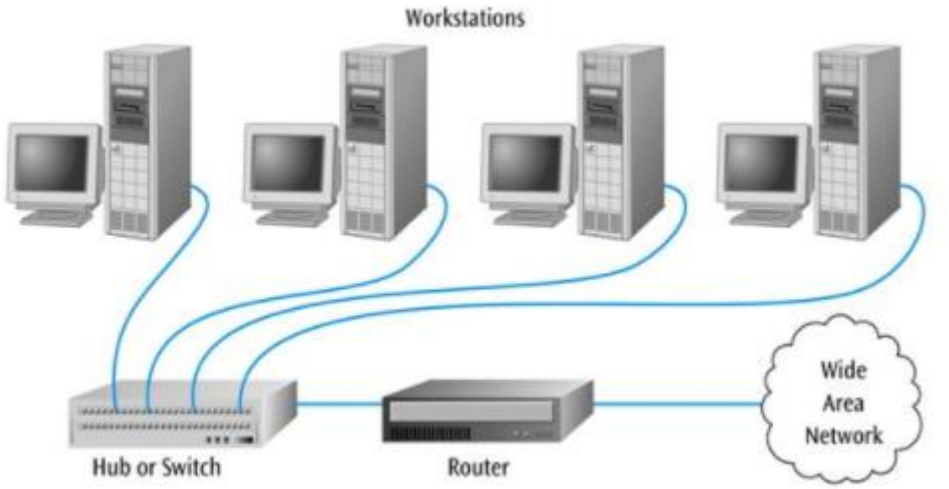
Tällaisesta asennuksesta on luonnollisesti niin hyötyjä kuin myös haittoja. Selkeimmät hyödyt ovat nopea tiedonsiirto laitteiden välillä ja resurssien tehokas jakaminen. Tämä pitää sisällään laitteiden ja sovellusten yhteisen käyttämisen, mikä voi käsittää muun muassa jaetun tietokannan tai vaikka vain tulostimen liittämisen useampaan työasemaan. (White 2011, 199.)

Lähiverkon haitat puolestaan lukeutuvat ylläpidon haasteisiin, missä ne kohdistuvat erityisesti yhteensopivuuteen ja lisensointiin. Mitä isommasta kokonaisuudesta on kyse, sitä

suuremmalla todennäköisyydellä jokin laite, sovellus tai niiden yhdistelmä ei ole yhteensopiva olemassa olevan asennuksen kanssa. Lisensoinnin kohdalla vuorostaan täytyy muistaa, että monilla ohjelmistoilla on erilliset versiot yhdelle ja useammalle käyttäjälle. (White 2011, 200.)

2.2 Lähiverkon aktiivilaitteet

Lähiverkon aktiivilaitteisiin luetaan kaikki verkkoon liitetyt laitteet niiden roolista huolimatta. Tämä joukko voidaan kuitenkin jakaa keskittimiin, päätelaitteisiin, palvelimiin ja kytkimiin sekä reitittimiin. Kuviossa 2 päätelaitteet liitetään keskittimellä tai kytkimellä lähiverkoksi, joka yhdistetään laajaverkkoon reitittimen kautta. (Koivunen 2010.)



Kuvio 2. Konfiguraatio lähiverkosta laajaverkkoon (White 2011, 11)

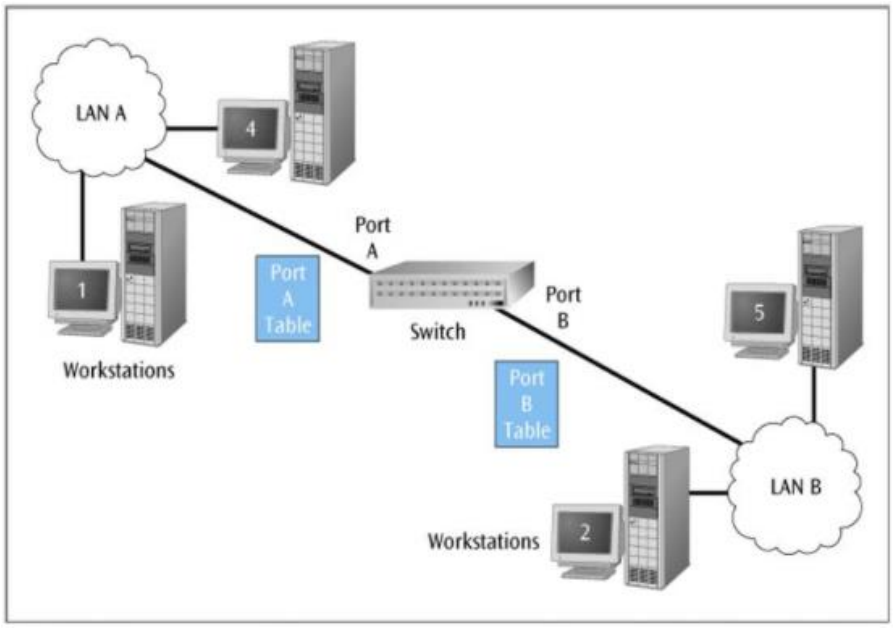
Keskitin on verkon komponentti, jonka toiminta perustuu toistimiin. Sen tehtävä on vastaanottaa dataa, joka lähetetään uudelleen kaikkiin siihen yhdistettyihin laitteisiin. Tällainen toiminta aiheuttaa paljon tietoliikennettä, mikä on selkeä haittapuoli erittäin aktiivisessa verkossa. Vastapainoksi asennus on yksinkertainen, koska se ei sisällä reititystä. (White 2011, 204.)

Lähiverkon päätelaitteet osio puolestaan sisältää kaikki käyttäjään suoraan liitoksissa olevat laitteet. Tämä kattaa siis muun muassa itse tietokoneet, matkapuhelimet ja tulostimet. Palvelimet puolestaan muodostavat oman osionsa, sillä niiden tehtävä on varastoida verkon ohjelmistoja ja hallinnointi-informaatiota. (White 2011, 7.)

2.2.1 Kytkin

Kytkintä käytetään samoissa tehtävissä kuin keskitintä, eli sillä liitetään laitteita lähiverkoiksi tai yhdistetään lähiverkkoja toisiinsa. Näiden laitteiden toimintaperiaatteet ovat kuitenkin erilaiset. Kytkimen tietoliikenne ohjataan eteenpäin datalle annetun ositteen mukaan, mikä vaati enemmän itse komponentilta mutta vähentää ruuhkautumista. (White 2011, 208.)

Tällöin avainasemassa on kytkimen verkkokortti (NIC, Network Interface Card). Verkkokortti tarkistaa liikenteen lähteen ja päämäärän, joita se vertaa oman verkkonsa osoitteisiin. Mikäli osoite kuuluu tähän alueeseen, data välitetään kohti päätelaitetta. Muussa tapauksessa informaatio johdetaan suoraan seuraavaan verkkoon, jonne kytkin olettaa datan olevan matkalla. (White 2011, 208.)



Kuvio 3. Kaksi lähiverkkoa yhdistävä kytkin omaa kaksi erillistä porttilistaa (White 2011, 210)

Kytkin kerää toimintaansa varten osoitetietoja ollessaan osa verkkoa. Esimerkiksi kuvion 3 kytkin aloittaa tyhjillä porttilistoilla A ja B, kun se kytketään kokonaisuuteen. Näitä listoja aloitetaan täyttämään sitä mukaa kun liikennettä saapuu komponenttiin. (White 2011, 209 - 210.)

Mikäli esimerkkitilanteessa työasema 2 lähettää tietoa työasemalle 5, sama lähetys päätyy myös kytkimeen. Tämän tiedon tunnisteiden avulla kytkin lisää työaseman 2 porttilistaan B. Samalla laite kuitenkin välittää tiedon eteenpäin lähiverkkoon A, koska työaseman 5 sijainnista ei ole informaatiota. (White 2011, 210.)

Mahdollinen vastauslähetys työasemalta 5 ei kuitenkaan päätyisi verkon B ulkopuolelle, koska sen osoitetiedot saataisiin listattua. Tällöin kytkimen näkökulmasta molemmat työasemat ovat osa portin B takaista verkkoa, eli tätä tiedonsiirtoa ei pidä välittää eteenpäin. (White 2011, 210.)

Kytkimet pystytään jakamaan sen perusteella, voidaanko niitä hallinnoida vai ei. Laitteesta riippuen konfigurointi voi tapahtua CLI:n, SNMP:n tai verkkokäyttöliittymän kautta. Yleisiä hallinnoinnin kohteita ovat porttien tilat ja virtuaalilähiverkot. Hallinnoimaton kytkin puolestaan on nopea ja yksinkertainen verkkoratkaisu, joka soveltuu juurikin yksinkertaisiin ja kevyisiin verkkoihin. (Wikipedia 2018a.)

2.2.2 Reititin

Reitittimen tehtävä on yhdistää vähintään kaksi tietoverkkoa toisiinsa. Käytännössä tämä voi tarkoittaa kahden lähiverkon yhdistämistä keskenään tai lähiverkon yhdistämistä laajaverkkoon ja sitä kautta internetiin. (White 2011, 4.)

Reitittimen toiminta perustuu erillisen reititysprotokollan varaan, näitä protokollia vuorostaan on useita erilaisia. Laitteeseen suunnattu tietoliikenne välitetään tämän protokollan ja laitteen reititystietojen avulla haluttuun päämäärään. (Wikipedia 2018b.)

Asennuksesta riippuen reititys on joko dynaaminen tai staattinen. Staattinen reititys pohjaa siihen, että reititystaulu luodaan kerralla kuntoon, minkä jälkeen sitä ei enää päivitetä. Dynaamisessa reitityksessä puolestaan reititystaulun sisältö vaihtelee laitteiden lähettämien tilapäivitysten mukaan. (White 2011, 296.)

Dynaaminen reititys on mukautuvaisempi vaihtoehto, mutta sen varomaton käyttö voi ruuhkauttaa verkkoa. Staattinen reititys on siis nopeasti katsottuna näistä kahdesta tehokkaampi valinta. Joustamattomuus on kuitenkin erittäin suuri haitta modernissa verkkoympäristössä, mikä voi pahimmassa tilanteessa hidastaa verkkoa ruuhkautumista enemmän. (White 2011, 296.)

Näistä haasteista voidaan siis helposti päätellä, että käytetty tekniikka riippuu asennuksen vaatimuksista. Verkkoa suunniteltaessa tulee suunnittelijan ottaa huomioon yhteyksien tarpeet ja yhdistellä ratkaisuja, jotta lopputulos olisi mahdollisimman optimoitu. (White 2011, 296.)

2.3 Tietoverkon arkkitehtuuri

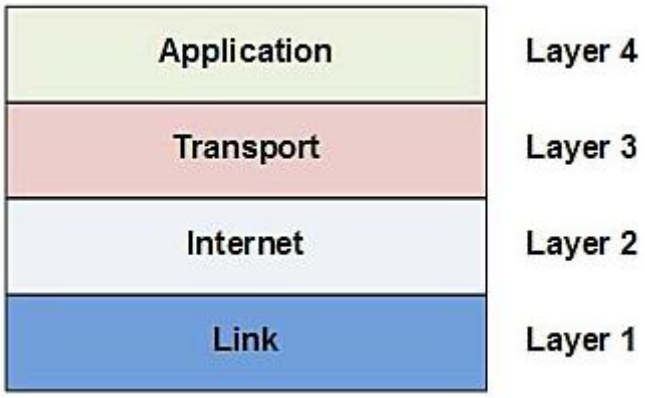
McCabe (2007) kuvaa verkon arkkitehtuuria kokonaisuuden päästä päähän ulottuvaksi rakenteeksi. Tämä struktuuri sisältää laitteiden sisäiset ja välilliset yhteydet, millä viitataan muun muassa osoittamiseen ja reititykseen. Verkon hallinnointi, suorituskyky ja turvallisuus luetaan myös osaksi kyseistä asetelmaa. (McCabe 2007, kappale 5.)

Osoittamis- ja reititysarkkitehtuurit keskittyvät verkkotasolle, mutta niillä on myös yhteyksiä laitetasolle. Hallinnointi, suorituskyky ja turvallisuus puolestaan ovat läsnä kaikilla tasoilla, mutta eivät samanlaisessa keskiössä kuin osoittaminen ja reititys. (McCabe 2007, kappale 6 - 9)

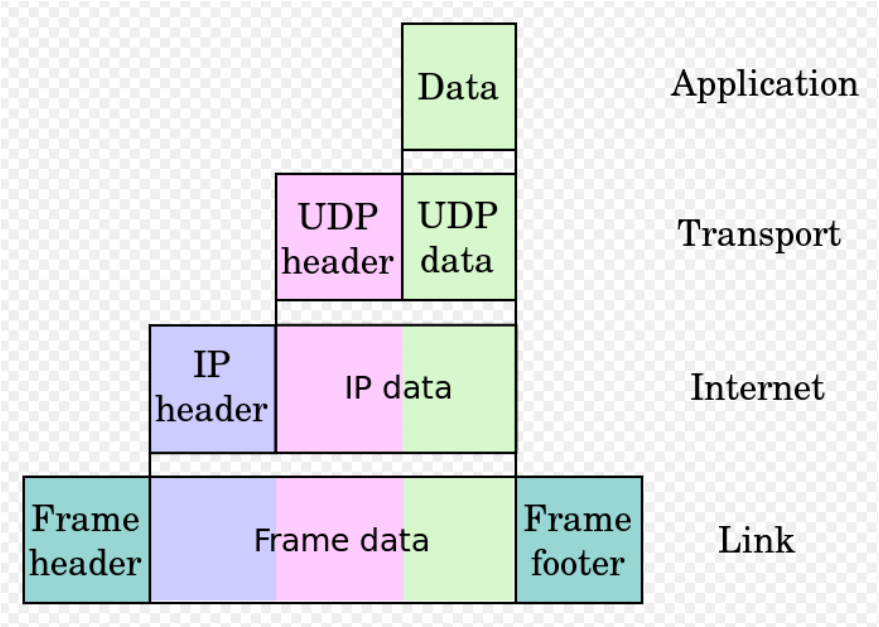
Puskakin (2000, 18 - 20) painottaa lähiverkon tietoliikenteen toiminnan ja sanomarakenteen merkitystä, jota määritellään erilaisilla kerrosmalleilla. Esimerkiksi TCP/IP-viitemalli oli yksi ensimmäisistä verkkoarkkitehtuureista, mutta kyseinen viitemalli näkee yhä käyttöä internetissä. Tämän lisäksi se on vaikuttanut selvästi seitsenkerroksisen OSI-malli syntyyn.

2.3.1 TCP/IP-viitemalli

Kuviossa 4 esitelty TCP/IP-viitemalli jakaa tietoliikenteen neljään kerrokseen (Wilkins 2012.). Puska (2000, 18) vaihtoehtoisesti kuvaa mallia kolmikerroksisena, jättäen liitännän mallin ulkopuolelle. White (2011, 17) puolestaan lisäisi fyysisen kerroksen mallin viidenneksi kerrokseksi. RFC 1122 on määritellyt tietoliikenteen kapseloinnin toimivan kuvion 5 mukaisesti, joten nelikerroksinen versio täyttää standardit. (Wikipedia 2018d.)



Kuvio 4. TCP/IP-malli (Wilkins 2012)



Kuvio 5. RFC 1122:n mukainen datan kapselointi (Burnett 2008)

Nelikerroksinen malli sisältää sovellus-, kuljetus-, verkko- ja peruskerroksen (Wilkins 2012.). Sovelluskerros (Application layer) avustaa verkon sovelluksia ja voi tilannekohtaisesti sisältää lisäyksiä, joihin muun muassa kryptaus lasketaan. Kuljetuskerros (Transport layer) hyödyntää mallin nimen mukaisesti TCP:a (Transmission Control Protocol) tietoliikenneyhteyden ylläpitämiseen. (White 2011 18 - 19.)

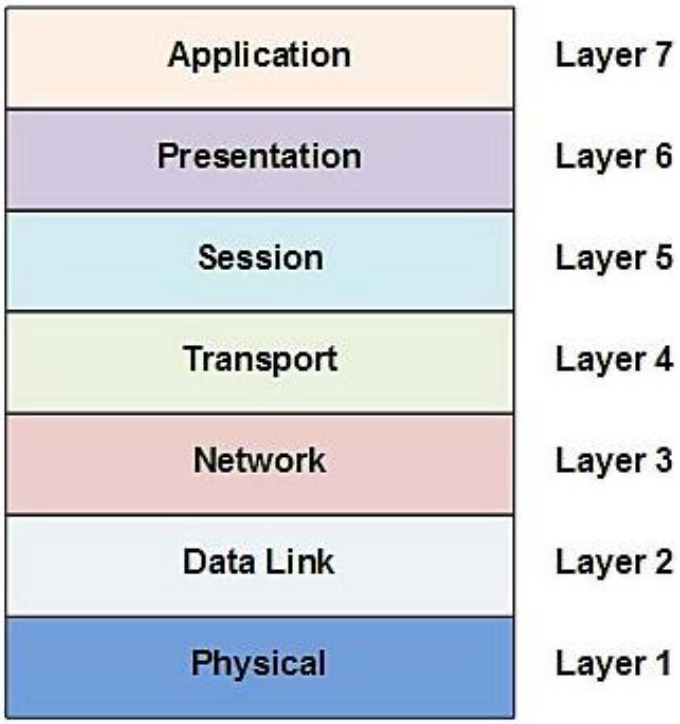
Verkkokerros (Internet layer) käyttää IP:aa (Internet Protocol), jolla lähetys pilkotaan standardikokoisiksi datapaketeiksi (White 2011, 19). Peruskerros (Link Layer) vuorostaan on viitemallin heikoiten määritelty kerros. Syy tähän on se, että malli vain olettaa IP:n alapuolella olevan jonkin rajapinnan, joka pystyy välittämään paketit. Lähiverkon tapauksessa tämä rajapinta on Ethernet. (Wikipedia 2018d.)

2.3.2 OSI-malli

Kuvion 6 esittämä seitsenkerroksinen OSI-malli koostuu seuraavista osista:

- sovelluskerros (Application – Layer 7)
- esitystapakerros (Presentation – Layer 6)
- yhteysjaksokerros (Session – Layer 5)
- kuljetuskerros (Transport – Layer 4)
- verkkokerros (Network – Layer 3)

- siirtoyhteyskerros (Data Link – Layer 2)
- fyysinen kerros (Physical – Layer 1). (Puska 2000, 19 – 20.)



Kuvio 6. OSI-malli (Wilkins 2012)

Tämän mallin sovelluskerros toimittaa samaa virkaa kuin TCP/IP:n vastaava, eli verkon sovellukset toimivat sen sisällä. Kuitenkin kryptaus ja muut esitystavan määrittävät komponentit ovat saaneet oman kerroksen esitystapakerroksen muodossa. Yhteysjaksokerrosta käytetään yhteyksien muodostamiseen ja jaksottamiseen käyttäjien välillä, minkä lisäksi se luo varmistuspisteitä virhetilanteita varten. (White 2011, 20 - 21.)

Kuljetuskerros on vastuussa liikenteen eheydestä, mikä käytännössä tarkoittaa, että perille saapunut data on identtinen lähteneen datan kanssa. Tämä vaatii, että lähetyksessä ei ollut virheitä, saapumis- ja lähetysjärjestys vastasivat toisiaan ja kahdentumia ei sattunut. (White 2011, 22.)

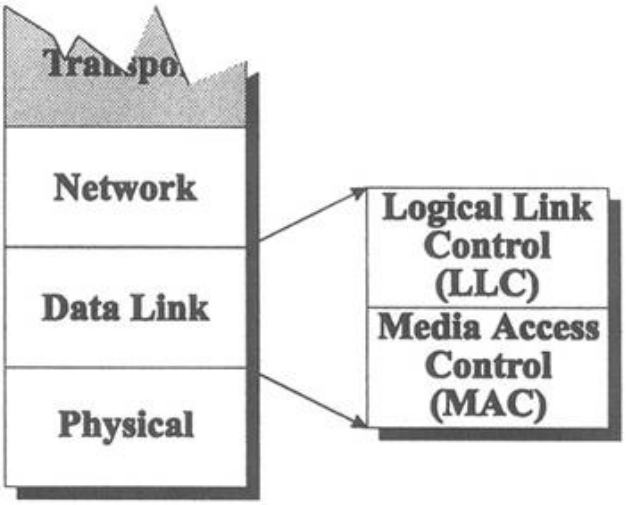
Verkkokerroksen tehtävä on avata, ylläpitää ja sulkea yhteyksiä verkon laitteiden välillä. Tällainen toiminta vaatii osoittamis- ja reititystietoja, joita kerros kerää lähettämällä kyselyjä omatoimisesti. Useimmissa lähiverkoissa data välitetään kaikille tahoille, jolloin tämä kerros jää melko suppeaksi. (White 2011, 22.)

Siirtoyhteyskerros muuttaa verkkokerroksen datan kehyksenä tunnettuun yksikköön, jollaisena se välitetään luotettavammin haluttuun kohteeseen. Kehys sisältää tiedon omasta aloitus- ja lopetuspisteestään, minkä lisäksi siinä on tilaa hallinta- ja osoittamistiedolle. (White 2011, 22.)

Tiedonkuljetuksen suunnasta riippuen mallin viimeinen tai ensimmäinen osa on fyysinen kerros. Fyysinen kerros huolehtii bittien siirrosta käytössä olevien kanavien kautta. Tästä johtuen kerros määrittelee käytetyn koodauksen tai modulaation tekniikan. (White 2011, 22.)

2.4 IEEE 802

802.x-lähiverkkostandardien kehitys aloitettiin jo 1980-luvulla IEEE:n toimesta. Näillä standardeilla pyrittiin rajoittamaan valmistajakohtaisia toteutuksia ja luomaan yhtenäinen rajapinta erilaisille lähiverkoille. Kriteerit määrittelevät muun muassa millaisia kehyksiä ja mediavaihtoehtoja väylät käyttävät. (Puska 2000, 21.)



Kuvio 7. LLC-alikerros (Cummins, 2000)

IEEE 802:n yksi näkyvimmistä päätöksistä oli siirtoyhteyskerroksen jakaminen LLC- ja MAC-kerroksiin kuvion 7 mukaisesti. Syynä tähän jakoon oli OSI-mallin 2. kerroksen toiminnan selkeyttäminen. Tästä johtuen LLC ja sen looginen osoittaminen haluttiin erottaa omaksi osuudekseen. MAC-kerros kuitenkin toimii yhä erittäin läheisesti fyysisen kerroksen kanssa, minkä takia näiden kerrosten raja on häilyvä. (White 2011, 225.)

2.5 Verkkoprotokollat

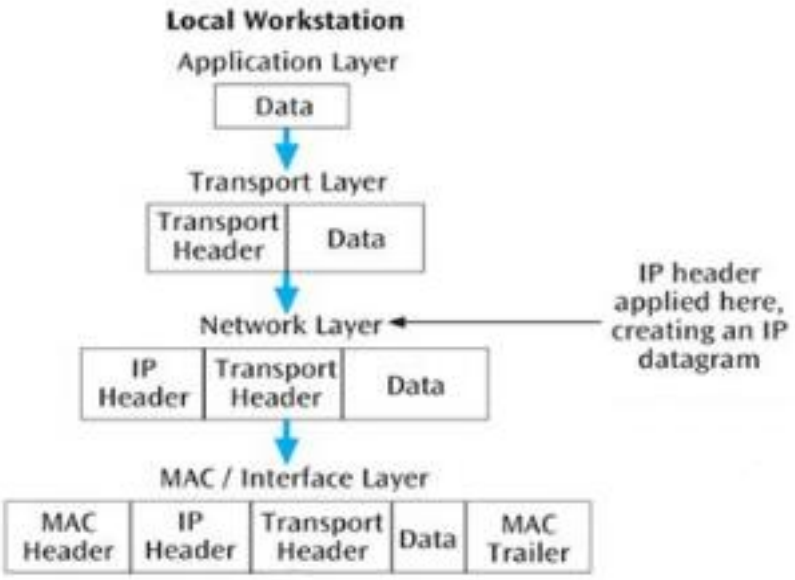
Verkkoprotokollat ovat virallisia normeja, jotka määrittävät, miten vähintään kaksi päätelaitetta kommunikoivat keskenään verkon yli. Protokollien tehtävä on hallita tämän yhteyden prosesseja, välitettyä dataa ja itse viestintää. (Techopedia 2018b.)

Tästä tehtävästä johtuen kaikki toiminta lähiverkosta internettiin ja sen yli toimiviin sovelluksiin luottaa verkkoprotokolliin. Kokonaisuutena verkko hyödyntää monia verkkoprotokollia ja usein samanaikaisesti, mistä johtuen käyttö määrittyy tilanteen mukaan. (White 2011, 309.)

White (2011, 309) listaa IP:n, TCP:n, ICMP:n, UDP:n ARP:n, DHCP:n ja NAT:n yleisimmiksi verkkoprotokolliksi. Tämän opinnäytetyön kannalta tärkeitä ovat listan IP ja UDP sekä sen ulkopuolelta SNMP ja TFTP. Kappaleessa kolme käsitellään myös IPsec- ja SSL-protokollia.

2.5.1 IP

Internet Protokolla (IP) kuljettaa dataa verkossa välittämällä ja reitittämällä IP data paketteja. Tämä tapahtuu lisäämällä IP-ylätunniste tietoliikenteelle kuljetuskerroksen ja verkkokerroksen välissä, kuten kuviossa 8. Tällöin tiedonsiirron kannalta olennainen informaatio on yhdessä määritellyssä osassa lähetystä. (White 2011, 310.)



Kuvio 8. Lähetettävän datan ylätunnisteen määrittäminen (White 2011, 311)

Ylätunnisteen informaatio kattaa paketin osoitetiedot, koon ja sen, milloin se luotiin. Tiedonsiirron aikana yksikön MAC- ja WAN-tiedot voivat vaihdella, mutta onnistuneen prosessin kohdalla paketin ylätunniste ja sisältö pysyvät muuttumattomina. (White 2011, 311.)

2.5.2 UDP

UDP (User Datagram Protocol) mahdollistaa tiedonsiirron kahden tahon välillä ilman yhteyden luomista. Tämän myötä protokolla ei ota kantaa yhteyden laatuun, pakettien järjestykseen tai niiden mahdolliseen vanhentumiseen. (White 2011, 317.)

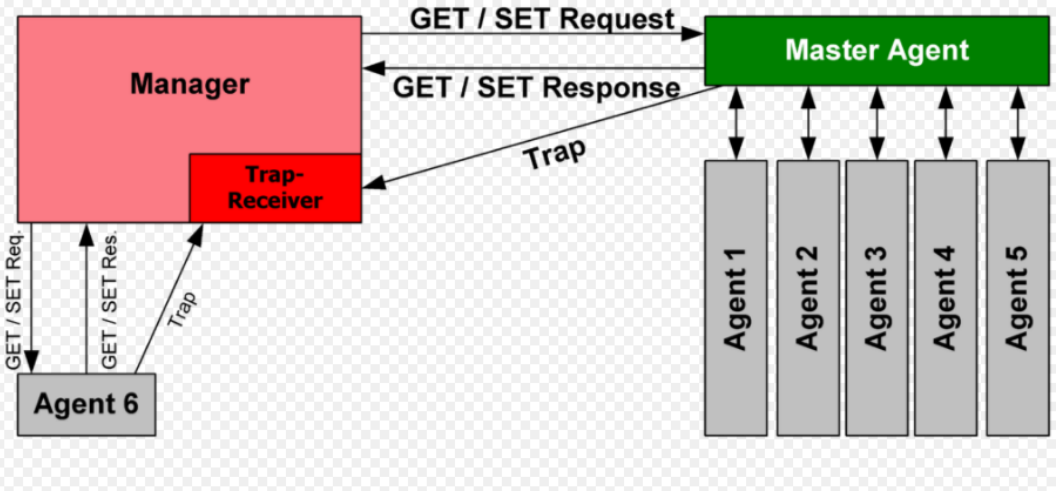
UDP ylätunniste sisältää vain neljä kenttää, jotka ovat: lähde, määränpää, pituus ja tarkistussumma. Tällainen järjestely, joka ohittaa alkukättelyn, on omiaan muun muassa DNS-pyyntöjen lähettämiseen. Tekniikkaa ei kuitenkaan voida soveltaa huolimattomasti, sillä vikasietoisuuden puute on selkeä haitta monille sovelluksille. (White 2011, 317.)

2.5.3 SNMP

SNMP (Simple Network Management Protocol) mahdollistaa tiedon saamisen hallinnoidun laitteen MIB (Management Information Base) tietokannasta. Tämä saavutetaan yleensä NMS:in (Network Management Workstation) lähettämien kometojen avulla, jotka välitetään juurikin SNMP:lla. Protokolla kuitenkin lainaa kuljetustapansa toiselta taholta, joka on usein UDP. (Allied Telesis 2015, 9.)

SNMP toimii vain kuuden erilaisen operaation avulla, mikä tekee siitä verrannollisesti yksinkertaisen tapauksen protokollien joukossa. Nämä komennot ovat get, get-next, get-response, set, trap sekä version 2c get-bulk-request. Get-kommentojen tehtävä on hakea objektin tietoja MBI:sta. Kyseisen objektin sijainti ja koko määrittävät, mitä vaihtoehtoa NMS tulee käyttämään. (Allied Telesis 2015, 10 - 11.)

Set-komento puolestaan mahdollistaa objektin arvojen muuttamisen tietokantaan NMS:n avulla. Viimeisen operaation tehtävä on ilmoittaa työasemalle, mikäli tietokannassa tapahtuu jotain tavallisesta poikkeavaa. Tällaisessa tilanteessa MIB:ssa sijaitseva sovellus lähettää trap PDU:in NMS:lle. (Allied Telesis 2015, 10 - 11.)



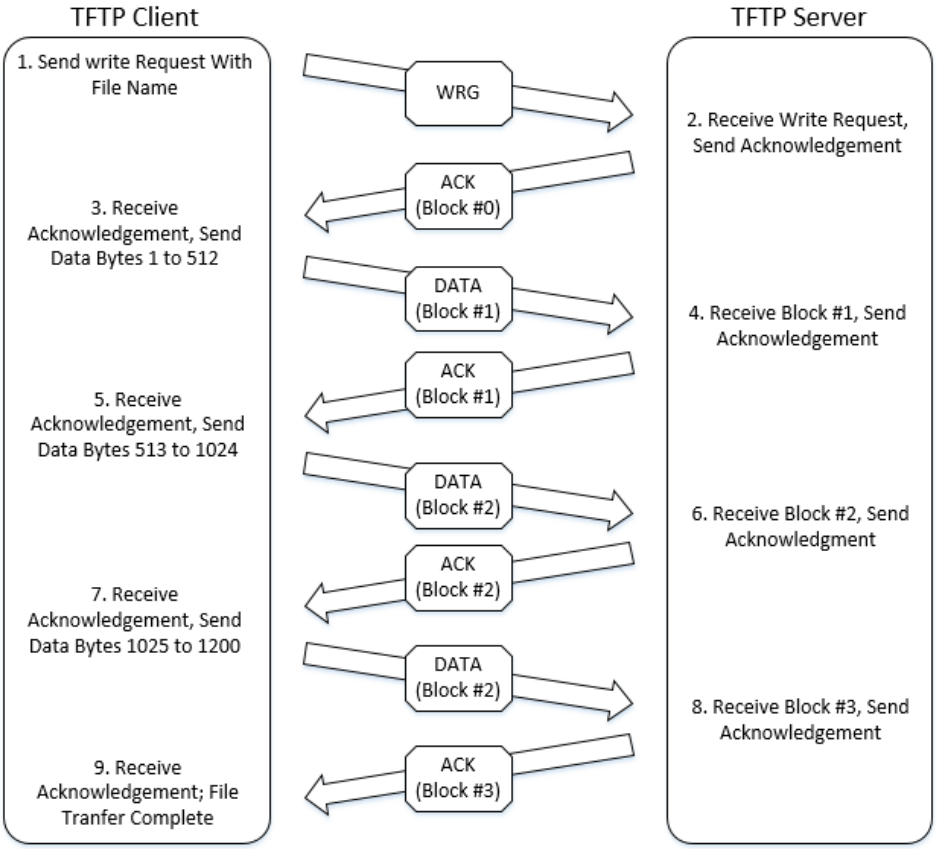
Kuvio 9. SNMP:n toimintaperiaate (Bretz 2006)

Kuviossa 9 hahmotetaan protokollan perustoiminta. Manager (NMS) lähettää Get- / Set-komentoja agenteille, eli hallinnoitavissa laitteissa sijaitseville sovelluksille. Nämä agentit puolestaan lähettävät vastaavia vastauksia komentoihin sekä tarpeen vaatiessa trap yksiköitä. (Wikipedia 2018c.)

2.5.4 TFTP

TFTP:n (Trivial File Transfer Protocol) mahdollistaa yksinkertaisen tiedonsiirron päätelaitteen ja etäkoneen välillä. Yksinkertaisen protokollasta tekee UDP:n hyödyntäminen, tunnistuksen puuttuminen ja yhden kanavan käyttö datan kuljettamiseen. (Egli 2015, 3.)

TFTP on pyyntöön ja kuittaukseen perustuva prosessi, jossa jokainen paketti kuitataan erikseen ennen kuin seuraava lähetetään. Egli (2015, 3.) nimeää protokollan moderniksi käyttötarkoitukseksi uuden koodin lataamisen verkkolaitteisiin. Esimerkiksi NETLAB+ hyödyntää TFTP:a juuri tällä tavalla.



Kuvio 10. TFTP:n kirjoitusprosessi (mukaillen Kozierok 2005)

Kuviossa 10 esitellään protokollan kirjoitusprosessi, eli tiedon siirto päätelaitteesta palvelimelle. Toimitus alkaa päätelaitteen kirjoituspyynnöllä, mihin palvelin lähettää kuittauksen. Tämä lähetys ja kuittaus kierre jatkuu koko siirron ajan, kunnes haluttu informaatio on saatu palvelimelle. (Egli 2015, 7.)

Kirjoitusprosessi palvelimelta päätelaitteelle toimii vastaavalla tavalla, eli pelkät nimet päikseen vaihtamalla kuvio yhdeksän voisi kuvata sitäkin. Lukuprosessi puolestaan alkaa lukupyynnöllä, mihin toinen osapuoli vastaa dataa lähettämällä. Tällöin toiminnan aloittajan vastuulla on lähettää kuittaus, kun paketti saapuu perille. (Egli 2015, 6 - 7.)

3 ETÄKÄYTTÖ

3.1 Etäkäytön määritelmä

Etäkäytöllä tietotekniikassa kuvataan tilannetta, jossa käytetään jotain elementtiä muuten kuin paikallisesti. Tällaisessa toiminnassa kohteeseen luodaan yhteys lähiverkon (LAN), laajaverkon (WAN) tai virtuaalisen erillisverkon (VPN) yli, mikä mahdollistaa esimerkiksi työntekijän käyttää työkonettaan tai työpaikkansa verkkoa kotoa käsin. (Techopedia 2018a.)

Alkujaan etäkäyttö toteutettiin dial-up modeemien avulla. Kyseinen lähestymistapa kuitenkin osoittautui kalliiksi, erityisesti kaukopuhelujen ja muiden lisämaksujen takia. Tästä johtuen monet yritykset alkoivat hyödyntää menetelmiä, joissa julkista verkkoa käytettiin internetin yli. Kysynnän kasvu johti luonnollisesti teknologian kehittymiseen, mikä on lisännyt huomattavasti etäkäytön joustavuutta ja tuvallisuutta. (PaloAlto 2018b.)

Käytännön esimerkkinä etäkäytön hiomisesta on sen käyttämien protokollien parantelu. Etäkäyttö on pitkään hyödyntänyt OpenSSH protokollaan rimana sen yksinkertaisuuden, nopeuden ja turvallisuuden takia. Langattomien yhteyksien käytön yleistyessä, tätä osa-aluetta nähtiin tarpeelliseksi hioa. Seurauksena syntyi mobile shell (Mosh), joka toimii edeltäjäänsä paremmin korkean verkkoviiveen omaavissa ympäristöissä kuten 4G verkoissa. (Geerling 2015.)

3.2 Remote Access Service

Remote Access Service (RAS) termin otti ensimmäisenä käyttöön Microsoft, joka viittasi käsitteellä Windows NT:n sisäänrakennettuihin etäkäyttötyökaluihin. Termi on kuitenkin ajan myötä jalostunut kuvaamaan mitä tahansa laitteiston ja ohjelmiston yhdistelmää, joka mahdollistaa etäyhteyden vaatimien apuvälineiden käytön ja tiedonsiirron. Tätä etäkäytön tapaa sovelletaan hyvin usein IT-tukipalveluissa, jotta käyttäjää voidaan avustaa pitkästäkin välimatkasta huolimatta. (COLMAN IT 2017.)

Nykyään Microsoft RAS on suunnattu ohjelmoijille, jotka haluavat luoda etäkäytettäviä sovelluksia. Palvelu mahdollistaa Windows-käyttöjärjestelmän omaavan laitteen liittämisen lähiverkon palvelimeen. Tällainen järjestely kuitenkin edellyttää ympäristöltä joko WAN-linkkiä tai VPN-yhteyttä. (Microsoft 2018.)

3.3 VPN

Julkisen verkon kanssa toimittaessa käyttäjän on turha toivoa, että hänen toimintansa olisi yksityistä. Tällaisen verkon tietoliikenne on nimensä mukaisesti julkista, jolloin kaikilla verkkoon pääsevillä tahoilla on mahdollisuus tarkastella tätä kommunikaatiota. Tässä kohtaa VPN astuu kuvaan suojaamaan yhteyden liikennettä niin tarkkailulta kuin myös häirinnältä. (PaloAlto 2018a.)

VPN (virtuaalinen erillisverkko) pohjaa toimintaan, jossa vähintään kaksi verkkoa yhdistetään julkisen verkon yli näennäisesti yksityiseksi verkoksi. Tällä tavalla voidaan laitteiden sijainnista huolimatta hyötyä yksityisen verkon toimivuudesta, turvallisuudesta ja hallinnasta. (Wikipedia 2018e.)

Tekniikkaa voidaan käyttää kahteen erilaiseen toteutustapaan, jotka ovat VPN etäyhteys (VPN remote access) ja reitittimien välinen VPN-yhteys (router-to-router VPN). Ensimmäinen vaihtoehto toimii verkkoon erikseen asennetun tietokoneen ja sen salauksen avulla. Jälkimmäisessä tapauksessa VPN luodaan reitittimien välille, jolloin oletuksena valmistajan ohjelmisto hoitaa yhteyden ylläpidon. (Koulutus- ja konsultointipalvelu KK Mediat 2018.)

Yhteensopivuus voi kuitenkin olla ongelma reitittimien varaan rakennetussa toteutuksessa, sillä tällaiset ratkaisut ovat perukseltaan valmistajakohtaisia. Tämän myötä erillisiin koneisiin luottava VPN etäyhteys soveltuu luontaisesti useampaan tilanteeseen, mikä voidaan laskea selkeäksi eduksi. (Koulutus- ja konsultointipalvelu KK Mediat 2018.)

VPN-yhteyden tietoliikenne kulkee internetin läpi tunnelointiprotokollan välityksellä. Tämän protokollan tehtävä on kryptata ja kapseloida tämä data, joka tarkistetaan AAA-palvelimen avulla. Palvelin todentaa käyttäjän, valtuuttaa yhteyden ja kirjaa ylös yhteyden aikana tapahtuvan toiminnan. (PaloAlto 2018a.)

Yleensä VPN-yhteydet voidaan jakaa kahteen ryhmään niiden käyttämän protokollan mukaan, jotka ovat IPsec ja SSL. IPsec pohjaa jonkin tahon tarjoamaan ohjelmistoon, joka mahdollistaa yhteyden. SSL puolestaan käyttää web-selainta välipintana VPN yhteyden luomiseksi. (PaloAlto 2018b.)

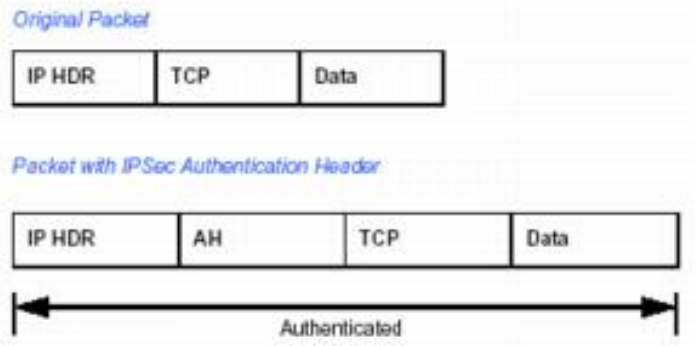
3.3.1 IPsec

IPsec-protokollat ovat internetin ytimenä toimivan Internet Protokollan lisäyksiä, joiden avulla voidaan välittää kryptauksella suojattuja datapaketteja. Tällöin käytetään erityisiä

ylätunnisteita, jotka ilmaisevat millaisesta kryptauksesta on kyse sekä mitä salauksen purkamiseen vaaditaan. Tässä osiossa tullaan käsittelemään toiminnalle olennaiset AH, ESP ja IKE protokollat. (Frankel 2001, 2-3.)

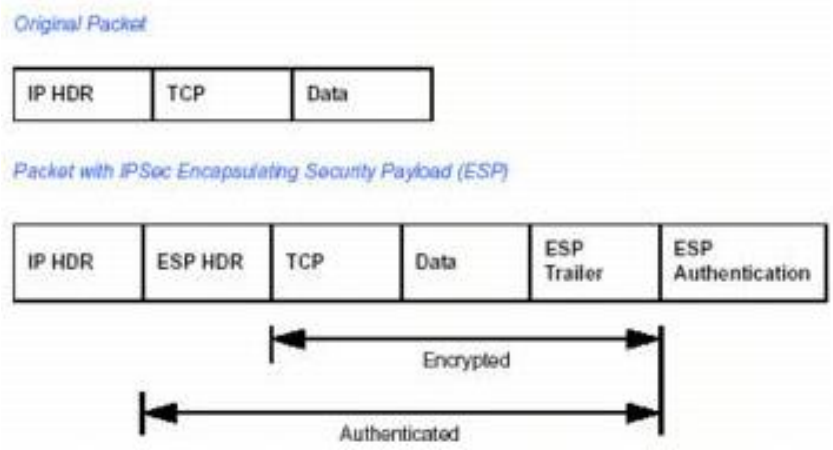
Näillä protokollilla on kolme selkeää päämäärää: tunnistus, eheys ja salaus. Tunnistuksella varmistetaan, että vastaanotettu tieto on väitetystä lähteestä. Tietoliikenteen eheydellä puolestaan taataan, että paketin sisältö ei ole muuttunut siirron aikana. Lopuksi salauksella huolehditaan siitä, ettei joku ulkopuolinen taho ole voinut suoraan lukea välitettyä tietoa. (NETGEAR 2005, 2-2.)

Authentication Header (AH) on tunniste, jolla voidaan tunnistaa datan lähettäjä sekä viestin sisällön eheys (kuvio 11). Tällä tekniikalla voidaan myös estää viestin lähettäminen useammin kuin kerran. (Frankel 2001, 15 - 16.) AH kuitenkin kompuroi salauksen suhteen, sillä viestin lähettäjä ja vastaanottaja ovat julkista tietoa. Tätäkin suurempi vaara ilmenee, jos viesti saadaan siepattua, koska se on tuolloin suoraan luettavissa. (NETGEAR 2005, 2-4.)



Kuvio 11. AH-tunniste (NETGEAR 2005, 2-4)

Encapsulation Security Payload (ESP) tarjoaa samat edut kuin AH, mutta lisää niihin kaksi varsin olennaista ominaisuutta. Ensiksi ESP salaa viestin sisällön, jolloin valtuuttamaton taho ei voi lukea sitä. Toiseksi protokolla pystyy estämään salakuuntelijoita määrittämästä mitkä tahot viestittävät keskenään ja kuinka paljon (kuvio 12). Jälkimmäinen suojaus toimii kuitenkin vain tunneloinnin yhteydessä, minkä takia se ei ole vakio-ominaisuus. (Frankel 2001, 41 - 42.)



Kuvio 12. ESP (NETGEAR 2005, 2-3)

Kolmikon viimeistä protokollaa varten on tarpeen valottaa käsitettä SA (Security Association). SA on summaus verkon laitteiden välisestä yhteydestä turvallisuuden suhteen, mikä määrittää käytettävät turvallisuus palvelut. Tämä käytäntö neuvotellaan istuntokohtaisesti, minkä takia prosessi yleensä automatisoidaan IKE:n avulla. (Cisco Press 2002.)

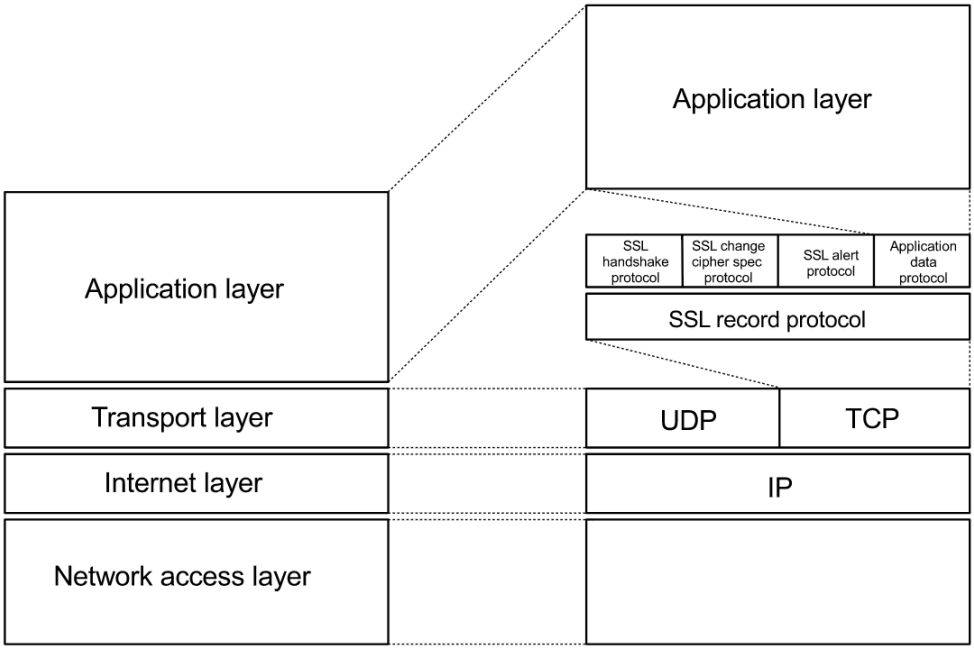
IKE (Internet Key Exchange) protokolla hallinnoi SA järjestelyä ja lukuavainten vaihtoa lähettäjän ja vastaanottajan välillä. Lukuavainten tehtävä on huolehtia siitä, että vain nämä tahot voivat päästä käsiksi lähetettyyn tietoon. Esimerkiksi ESP salattu viesti on lukukelvoton ilman sopivaa avainta. (NETGEAR 2005.) Prosessi itsessään on kaksivaiheinen neuvottelu, jonka aikana monivaiheisesti luodaan ISAKMP SA ja IPsec SA laitteiden välille. (Frankel 2001, 87 - 88)

3.3.2 SSL

SSL (Secure Sockets Layer) on käyttäjä- ja palvelinprotokolla, joka pyrkii tarjoamaan perusturvallisuuden tietoliikenteelle. Toteutuksen palvelut jaetaan tunnistusta, yhteyden luottamuksellisuutta ja liikenteen eheyttä vahvistaviin ominaisuuksiin. Protokolla ei kuitenkaan mahdollista välitetyn tiedon vahvistamista myöhemmin lähettäjän tai lähetyksen tietojen avulla, mikä erottaa sen S-HTTP:sta ja XML:stä. (Oppliger 2016, 21 - 22.)

SSL toimii OSI-mallin kuljetuskerroksella, joten protokollan välittämä liikenne on yhteyskohtaista (sockets-oriented). Tästä johtuen kaikki sen kuljettama data on suojattu samalla tavalla. Mikäli osaa tiedosta pitäisi eritellä tai vahvistaa, tarvitaan tähän sovelluskerroksen apua HTTP:n muodossa. (Oppliger 2016, 22 - 23.)

Protokollaa voidaan kuvailla epävirallisena kerroksena kuljetus- ja sovelluskerrosten välissä (kts. kuvio 13), jolla on kaksi tärkeää tehtävää. Ensimmäiseksi SSL:n täytyy luoda turvallinen yhteys tahojen välille, mikä vaatii tunnistuksen ja luottamuksellisuuden. Toiseksi sen velvollisuus on kuljettaa korkeamman kerroksen protokollatietoa lähettäjältä vastaanottajalle. Tämä välitys saavutetaan hajottamalla data pienempiin osiin, jotka vuorostaan puretaan, tunnistetaan ja avataan päämäärässä. (Oppliger 2016, 22 - 23.)



Kuvio 13. SSL ja sen alikerrokset sekä protokollat (Oppliger 2016, 23)

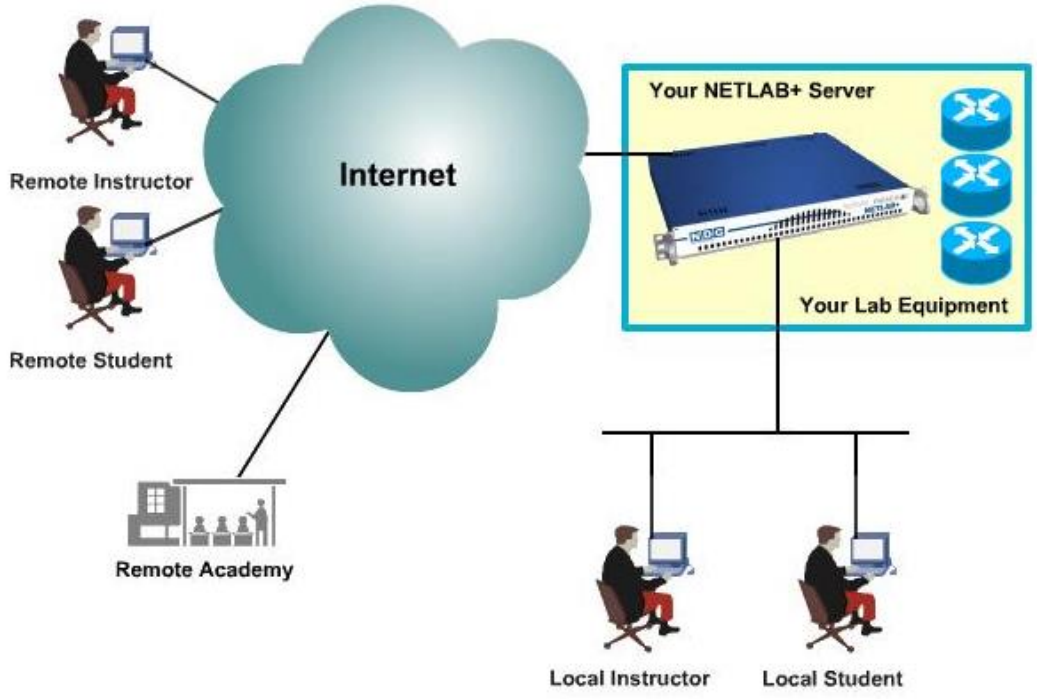
SSL version 3.0 jälkeen sen kehittäjä Netscape luovutti protokollan IETF-standardointiorganisaatiolle. Tämän seurauksena salausprotokollan nimi vaihdettiin TLS:ksi (Transport Layer Security) (Wikipedia, 2018c.). TLS:n rakenne on nimenmuutoksesta huolimatta identtinen SSL:n kanssa. Vuonna 2008 julkaistun TLS 1.2 on RFC:ssa määrätty korvaamaan tätä vanhemmat SSL ratkaisut. (Oppliger 2016, 91.)

4 NDG NETLAB+

4.1 NETLAB+

NETLAB+ on Network Development Group:in (NDG) kehittämä internetpohjainen verkkolaboratoriojärjestelmä, jolla pyritään tehostamaan tietoliikennetekniikan opetusta. Järjestelmä toimitetaan verkkosovelluksena, joka ei suoraan vaadi käyttäjältä aiempaa kokemusta UNIX:sta, verkkopalvelimista tai järjestelmänhallinnasta. (NDG 2009, 3.)

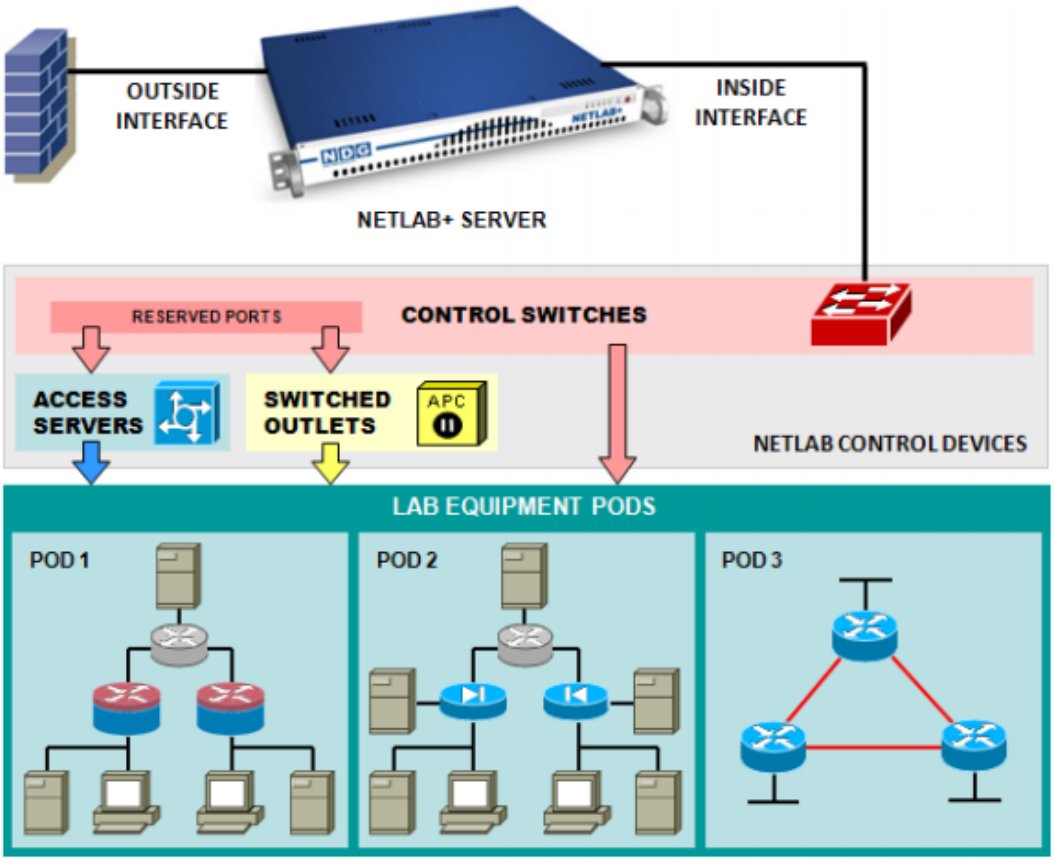
Sovelluksella luodaan turvallinen harjoitteluympäristö, jossa käyttäjät voivat kuitenkin konfiguroida ja olla vuorovaikutuksessa laitteisiin. Tämä saavutetaan sijoittamalla laitteet NETLAB+ palvelimen taakse, jolloin ne eivät ole suojattomasti esillä julkisessa verkossa (kuvio 14). Palvelu myös säästää aikaa hoitamalla tai suoraviivaistamalla monta askaretta, kuten konfiguraatioiden latauksen ja laitteiden tyhjentämisen harjoituksen jälkeen. (NDG 2009, 3.)



Kuvio 14. NETLAB+ yleiskuva (NDG 2009, 4)

Palvelin toimii välityspalvelimena, jonka läpi kaikki yhteydet kulkevat. Tämä tarkoittaa sitä, että kaikki verkkoliitäntöjen läpi kulkeva liikenne välitetään reitittämisen sijaan. Kokonaisuuden toiminnan kannalta kriittinen komponentti on palvelimeen yhdistetty hallintataso.

Hallintotaso on vastuussa laitteiden välisistä yhteyksistä, käyttäjän konsoliyhteyksistä ja virran jakamisesta. Kuvio 15 pyrkii selventämään tätä asennusta. (NDG 2009, 3.)



Kuvio 14. NETLAB+:n tasot (NDG 2009, 53.)

NETLAB+ listaa suurimmiksi eduikseen aikataulun ja tilan vapauttamisen, millä viitataan etäkäytön tarjoamiin hyötyihin sekä opetusympäristöön käsiksi pääsyyn vuorokauden ympäri. Tähän tähtäävät ominaisuudet voidaan jakaa käytännön, hallinnollisiin ja ylläpidollisiin palveluihin. (NDG 2009, 5 - 7.)

4.2 Järjestelmän käytännön palvelut

Käytännön osio palveluista kattaa laitesolut, laboratorioyhteyden, etäkoneet ja vuorottajan. Laitesolu on ennalta määritelty laitteistokokonaisuus, jonka käyttäjä varaa käyttöliittymän kautta. Kyseessä on looginen ja fyysisesti yhteen liitetty kokonaisuus, joka kuitenkin nähdään ja varataan yhtenä resurssina. (NDG 2009, 8.)

Laboratorioyhteys toimii järjestelmän käyttöliittymänä, jonka alle lukeutuvat topology-, action-, status-, connections-, load- ja save- sekä exercise-välilehdet. Näiden välilehtien avulla käyttäjä voi konfiguroida ja tarkkailla harjoituksessa käytettäviä laitteita; tarpeen

mukaan konfiguraatiot voidaan myös ladata aiemmasta käyttökerrasta tai tallentaa tulevaa varten. (NDG 2009, 9 - 20.)

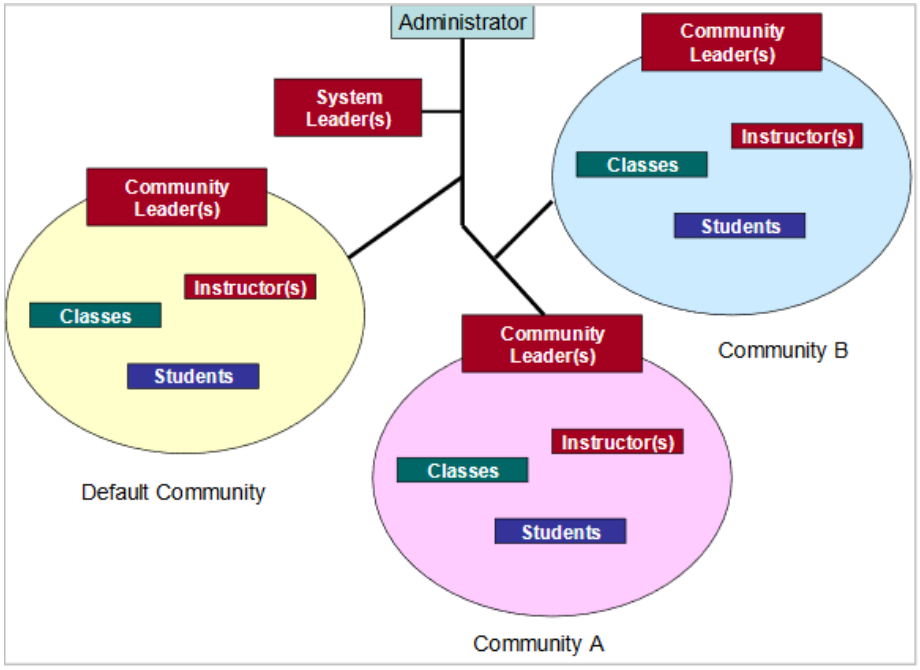
Etäkoneet palvelu sallii tietokoneiden lisäämisen laitesoluihin. Tämän asennuksen myötä kone on perukseltaan NETLAB+:n hallinnassa, mikä helpottaa sen käyttöä sovellusten, palomuurien ja yhteiskäytön suhteen. NETLAB+ suosii virtuaalikoneiden käyttöä mutta se voi tämän lisäksi hallinnoida erillisiä fyysisiä koneita. Täysin itsenäisen laitteen liittäminen on myös vaihtoehto mutta tuolloin käyttömahdollisuudet laskevat pelkän vuorovaikutuksen tasolle. (NDG 2009, 21 - 22.)

Vuorottaja on käytännön osuuden kasassa pitävä voima. Tämä sovellus allokoi järjestelmän resurssit käyttöön niiden varaustyypin ja ajan perusteella. Laitteisto voidaan varata luokkaa, ryhmää tai yksittäistä käyttäjää varten, minkä lisäksi ohjaaja voi tehdä varauksen itselleen tai liittyä oppilaana mukaan. (NDG 2009, 23 - 24)

4.3 Hallinnolliset palvelut

NETLAB+:n hallinnolliset palvelut edesauttavat järjestelmän käytössä ja tukevat opetusta. Näihin ominaisuuksiin lukeutuvat yhteisön, luokan ja tilien sekä tiedostojen hallinnointi. Tämän lisäksi ohjaajien käyttöön tarjotaan arviointia helpottavia työkaluja. Ylläpitäjän on myös mahdollista asentaa kokonaisia Cisco Networking Academyn opinto-ohjelmia yhteisön käyttöön. (NDG 2009, 25.)

Yhteisö NETLAB+:n kohdalla viittaa tiettyyn ryhmään, jonka yksi tai useampi ohjaaja, osallistuvat oppilaat ja kyseisen toteutuksen oppitunnit muodostavat. Tällaisessa tilanteessa ohjaajat voivat hallinnoida vain oman yhteisönsä oppilaita ja oppitunteja. Kyseinen järjestely mahdollistaa esimerkiksi useamman oppilaitoksen jakaa tai keskittää laitteistoa yhdessä. Kuviossa 16 valotetaan tämän järjestelyn hierarkiaa. (NDG 2009, 25)



Kuvio 16. NETLAB+ yhteisön hallinta (NDG 2009, 25)

Luokan, tilien ja tiedostojen hallinnointi palvelut ovat kaikki kevyempiä kokonaisuuksia. Luokan sisällä voidaan määritellä ryhmiä ja määrittää pääsyä oppimateriaaliin. Tilien avulla käyttäjät määritellään joko ohjaajiksi tai oppilaiksi. Tiedostojen kohdalla voidaan tarkastella, lisätä, muuttaa tai poistaa konfigurointi tiedostoja ja kansioita. (NDG 2009, 26 - 32)

Arvioinnin teon helpottamiseksi ohjaajilla on pääsy NETLAB+ Log Viewer työkaluun. Tämä apuväline näyttää lopullisen konfiguraation lisäksi suoritetun harjoituksen lokitiedoston, johon on tallennettu tehtävän aikana ajetut komennot. Tällä pyritään takaamaan, että ohjaaja voi vaivattomasti nähdä kuinka oppilas on edennyt tehtävässä ja vienyt suorituksen loppuun. (NDG 2009, 33 - 34)

4.4 Ylläpidolliset palvelut

Järjestelmän ylläpitäjälle tarjotaan monia ylläpidollisia palveluita, joita käytetään NETLAB+:n verkkokäyttöliittymän läpi. Kokonaisuuden laitteiston ylläpitoa varten on laitesolujen ja ohjauslaitteiden hallinnointityökalut. Toiminnan ja turvallisuuden takaamiseksi tarjolla on puolestaan automatisoitu päivitys, ajan synkronointi ja ohjelmiston varmuuskopiointi. Ylläpitäjä pystyy myös suunnittelemaan ja toteuttamaan uniikkeja harjoituksia ja soluja näiden palvelujen kautta. (NDG 2009, 35 - 50)

NETLAB+ tarjoaa tarkkaa tietoa kaluston niin fyysisistä kuin myös ohjelmistoasennuksista, mikä sisältää muun muassa kaapeloinnin ja sovellusversion. Käyttöliittymän kautta voidaan lisätä, testata ja poistaa laitteita tarpeen mukaan. Ohjauslaitteiden konfiguraatiota voidaan myös mukauttaa, mikä erottaa ne joustamattomista laitesoluista. (NDG 2009, 53 - 54)

5 ETÄKÄYTTÖJÄRJESTELMÄN LAAJENNUS

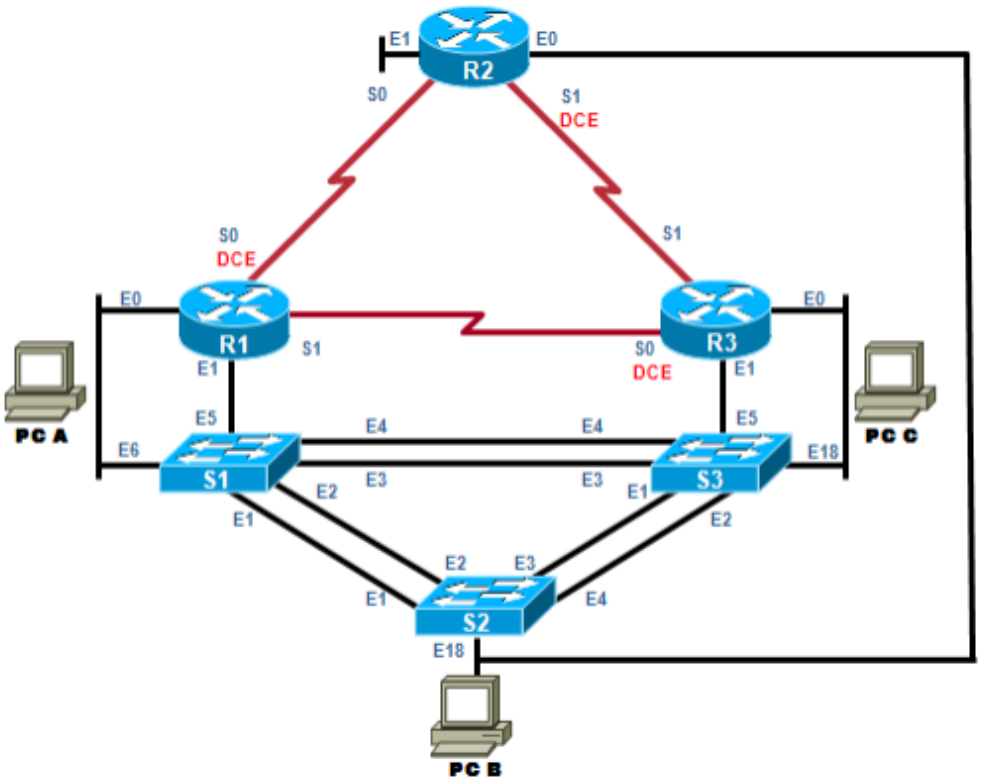
5.1 Järjestelmän laajennusvaihtoehdot

Opinnäytetyön käytännön osuuden painopiste oli Lahden ammattikorkeakoulun verkkotekniikan laboratorion etäkäyttöjärjestelmän laajennuksessa. Tämä kokonaisuus koostui neljästä osuudesta, jotka olivat:

- laajennusvaihtoehtojen vertailu
- asennuksen suunnittelu
- fyysinen asennus
- uusien laitesolujen testaaminen.

Oppilaitoksen tarpeiden ja käytössä olevien resurssien perusteella realistiset vaihtoehdot rajattiin kahteen. Ensimmäinen vaihtoehdoista oli NETLAB+:n akatemia version monikäyttöinen laitesolu. Vaihtoehto kaksi oli saman laitesolun sisarusversio, johon kuului samojen laitteiden lisäksi Cisco Systems Inc.:in Adaptive Security Appliance

5.1.1 Monikäyttöinen laitesolu

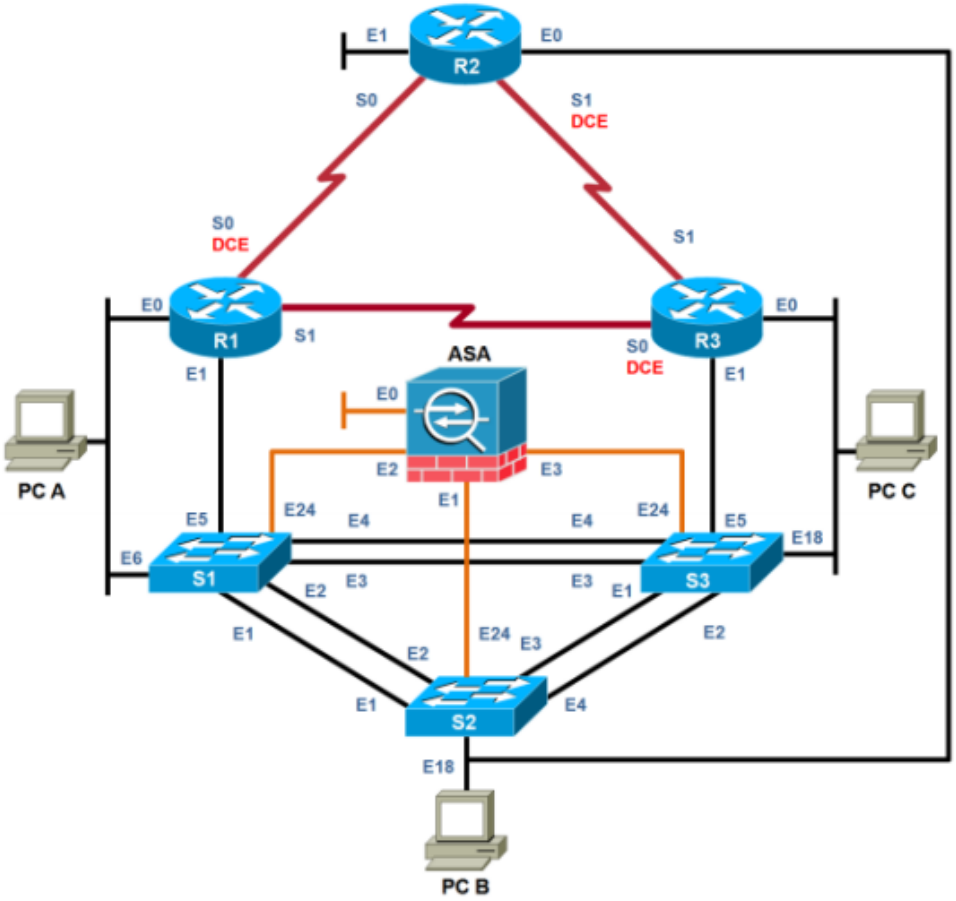


Kuvio 17. Monikäyttöinen laitesolu, MAP (NDG 2015, 3)

NETLAB+:n monikäyttöinen laitesolu koostuu kuvion 17 mukaisesti kolmesta reitittimestä, kolmesta kytkimestä ja kolmesta virtuaalikoneesta. Tällainen asennus tekee solusta erittäin joustavan, mikä käy ilmi sen nimestäkin. Solu on myös suunniteltu yhteensopivaksi valtaosan CCNA ja CCNP laboratorioharjoitusten kanssa.

Huomion arvoista on myös se, että perukseltaan järjestelmässä voi olla vain kahdeksan monikäyttöistä solua, mikä voi olla rajoittava tekijä. Tässäkin asennuksessa alkutilanne oli viisi laitesolua, mikä haluttiin laajentaa käsittämään täydet kahdeksan.

5.1.2 Monikäyttöinen laitesolu ASA:lla



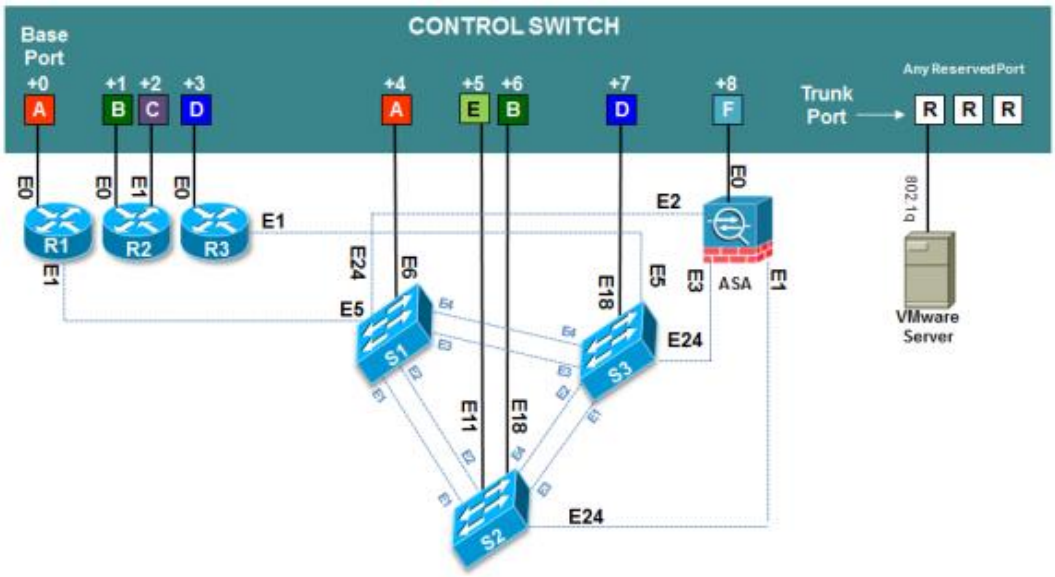
Kuvio 18. Monikäyttöinen laitesolu ASA:lla, MAPASA (NDG 2018, 3)

Kuten kuviosta 18 voi päätellä, MAPASA ei eroa paljoa standardista monikäyttöisestä laitesolusta. Aiemmin mainittu Cisco ASA on asennuksen ainoa fyysinen eroavaisuus. Komponentti liitetään solun kaikkiin kytkimiin, jotta kontrollikerros voi määrittää sen yhteydet harjoituskohtaisesti.

Laitesolu on suunniteltu sisarussolunsa tavoin yhteensopivaksi CCNA ja CCNP harjoitusten kanssa. MAPASA tukee perussolun harjoitusten lisäksi niitä tehtäviä, joihin kuuluu ASA komponentti. Tämän myötä asennuksen harjoituslista on standardisolua kattavampi.

5.2 Vaihtoehtojen vertailu

Vaihtoehtojen vertailussa tärkeää asemaan nousivat niiden tukemien harjoitusten lisäksi, mitä fyysisiä resursseja ne vaativat. Valittuja asennuksia tultaisiin lisäämään kolme kappaletta järjestelmään, joten kaikki kulut tulisivat myös kolminkertaisina.



Kuvio 19. MAPASA:n liitos kontrollikytkimeen (NDG 2018, 15)

Näistä vaatimuksista johtuen vertailun keskiössä olivat vastakkain MAPASA:n tarjoama laajempi harjoitusvalikoima, ja samaisen asennuksen lisäkulut verrattuna tavanomaiseen monikäyttöiseen laitesoluun. Kuvion 19 mukainen asennus standardiin (liite 1) verrattuna vaatisi lisäksi itse ASA komponentin, muutaman kaapeloinnin ja yhden virtalähdepaikan jokaista laitesolua kohden.

Lahden ammattikorkeakoulun toteuttamat CCNA kurssit ovat tähän mennessä kattaneet kaikki neljä osaa, ilman näitä ASA-harjoituksia. Pääasialliseksi syyksi tähän paljastui se, että tällaiset harjoitukset ovat erittäin harvassa CCNA:n kohdalla, eivätkä ne ole opintokokonaisuuden kannalta olennaisia tai pakollisia.

Tämän tiedon valossa MAPASA:n edut tässä kyseisessä laajennuksessa hävisivät sen haitoille. On kuitenkin hyvä ottaa huomioon, että tämä laajennus olisi voinut helposti olla kannattava.

Mikäli oppilaitos tarjoaisi nykyistä enemmän Ciscon kursseja, olisi mahdollisuus suorittaa ASA-harjoituksia selkeä etu. Toinen syy voisi standardi monikäyttöisten laitesolujen rajallinen määrä. Tämä asennus nosti LAMK:n järjestelmän juuri tuohon rajaan, minkä takia jatkossa laajennukset voivat hyvinkin nojata ASA:lla vahvistettuihin soluihin.

5.3 Laajennuksen suunnittelu

Kun laajennuksessa käytetty laitesolu oli selvillä, siirryttiin suunnitteluun. Tiedossa oli, että järjestelmään asennetaan kolme uutta monikäyttöistä laitesolua. Tästä voitiin alkaa laskemaan, mitä kaikkea tällainen laajennus tarkalleen vaati niin laitteiden kuin myös itse järjestelmän puolelta.

Fyysinen asennus sisälsi laitteiden osalta yhdeksän reititintä, kymmenen kytkintä ja kolme APC virtalaitetta. Tämän lisäksi listalle pääsivät laitteiden vaatimat kaapeloinnit, joista kuviot 20 ja 21 ovat esimerkkejä. Nämä kaapelointi esimerkit saatiin järjestelmään jo aiemmin asennetuista laitesoluista.

CABLE CHART FOR POD 6

R1 (Cisco 2801/2811 (S0/1/x))

CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet0/0	CAT-5 Straight Through	C/S 6	Port 1
FastEthernet 0/1	CAT-5 Straight Through	SW1	FastEthernet 0/5
Console	CAB-HD8-ASYNC	A/S 1	Port (tty) 0/1/14 Line 33 Octal cable P6
Power	Power Cord	SOD 5	Outlet 1
Serial0 DCE	Back-to-back serial cables	R2	Serial0 DTE
Serial1 DTE	Back-to-back serial cables	R3	Serial0 DCE

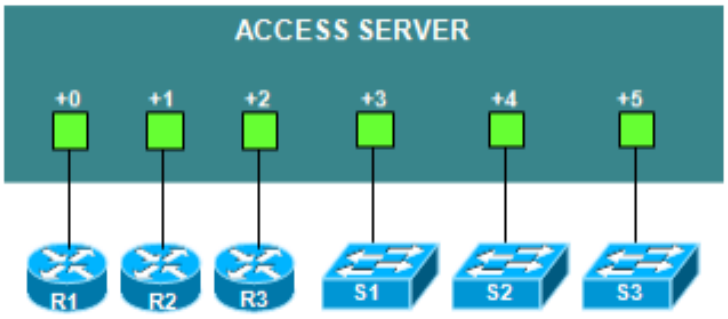
Kuvio 20. Laitesolun reitittimen R1 kaapelointi

S1 (Cisco 2960)			
CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet 0/1	CAT-5 Crossover	SW2	FastEthernet 0/1
FastEthernet 0/2	CAT-5 Crossover	SW2	FastEthernet 0/2
FastEthernet 0/3	CAT-5 Crossover	SW3	FastEthernet 0/3
FastEthernet 0/4	CAT-5 Crossover	SW3	FastEthernet 0/4
FastEthernet 0/5	CAT-5 Straight Through	R1	FastEthernet 0/1
FastEthernet 0/6	CAT-5 Crossover	C/S 6	Port 5
Console	CAB-HD8-ASYNC	A/S 1	Port (tty) 0/2/1 Line 36 Octal cable P1
Power	Power Cord	SOD 5	Outlet 4

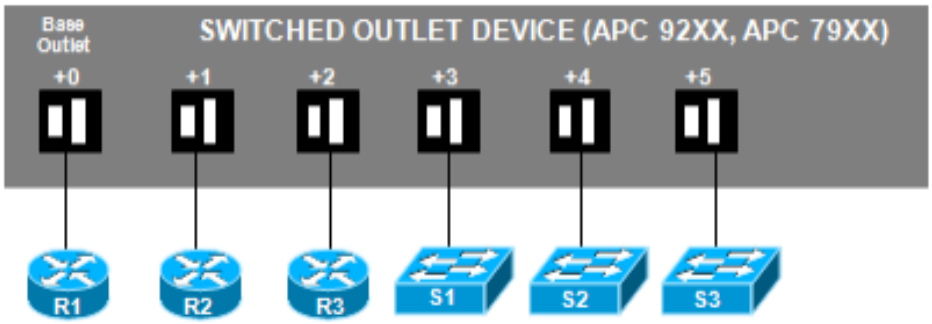
Kuvio 21. Laitesolun kytkimen S1 kaapelointi

Järjestelmän puolelta jokaista lisättävää solua varten täytyi varata resursseja kolmesta eri lähteestä. Ensimmäiseksi laitesolu tarvitsee kahdeksan porttipaikkaa kontrollikytkimestä (liite 1). Tässä kohtaa kävi myös selväksi, että järjestelmään täytyisi lisätä uusi kontrollikytkin laajennusta varten.

Toiseksi jokainen fyysinen laite täytyy liittää NETLAB+-yhteyspalvelimeen, mikä tarkoittaa kuutta paikkaa jokaista solua kohden (kuvio 22). Lopuksi järjestelmän hallitsemiin virtalähteisiin täytyy varata paikat komponenteille, kuten kuviossa 23.



Kuvio 22. Laitesolun vaatimat palvelin liitännät (NDG 2015, 15)



Kuvio 23. Laitesolun vaatimat virtayhteydet (NDG 2015, 15)

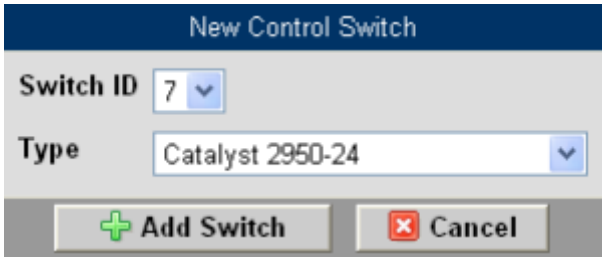
5.4 Laajennuksen toteutus

Asennukselle oli varattu oma laitekaappi, johon laitteet sijoitettiin seuraavaan järjestykseen: ensin virtalaitteet, seuraavaksi kontrollikytkin ja lopuksi laitesolut. Kytkennän helpottamiseksi ja selkeyttämiseksi solut kaapeloitiin yksi kerrallaan allekkain, eli kolme reititintä kolme kytkintä linjauksella.

Kytkennät voi ja kannattaakin tehdä valmiiksi suunnitelman mukaan, sillä kun laite tai kokonainen solu lisätään järjestelmään, täytyy kaikki laitesolut sammuttaa prosessin ajaksi. Tuolloin siis järjestelmän avulla ei ole mahdollista työskennellä. Tämä toiminta myös nollaa laitevaraukset, minkä takia se täytyy ajoittaa hyvin tai vähintään informoida käyttäjiä asiasta.

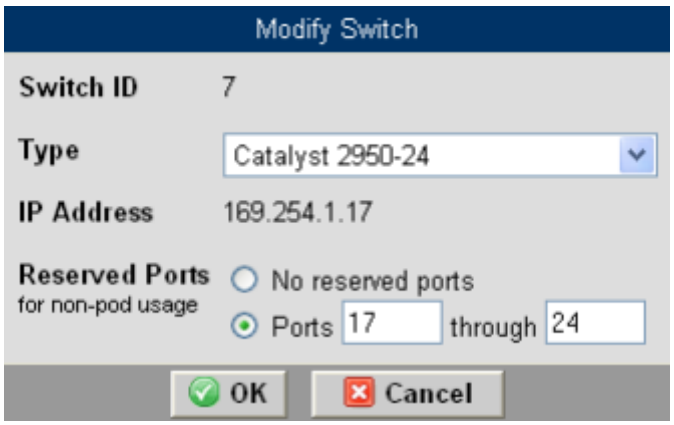
5.4.1 Kontrollikytkimen lisääminen järjestelmään

Kontrollikytkin lisätään järjestelmään nettikäyttöliittymän kautta. Tällöin edetään Control Devices -kuvakkeesta Control Switches -osioon. Tämän jälkeen valitaan Add a Control Switch -vaihtoehto. Seuraavaksi määritellään kuviossa 24 näkyvästä valikosta laitteen ID sekä tyyppi. Opinnäytetyön asennuksessa ID oli 6 ja laitteen tyyppi Catalyst 3550-24.



Kuvio 24. Uuden kontrollikytkimen määrittäminen

Seuraavaksi aukesi kuviossa 25 näkyvä kontrollikytkimen hallintavalikko. Tässä valikossa voidaan määrittää ne portit, joita käytetään muuhun kuin laitesolujen yhteyksiin. Kontrollikytkimen 6 kohdalla tällaisia portteja ei määritelty, sillä ne menivät kaikki solujen käyttöön.



Kuvio 25. Kontrollikytkimen hallintavalikko

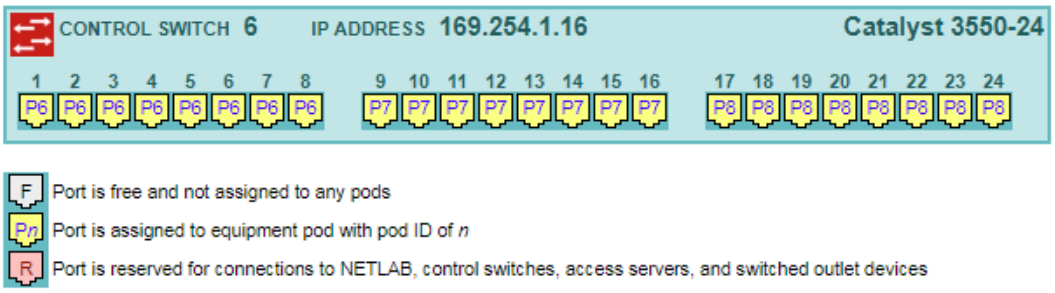
Ennen kuin kytkimeen voitiin tehdä viimeiset konfiguraatiot, täytyi muutaman asian olla kunnossa. NETLAB+ palvelimen ja kytkimen kuului olla päällä, kaapeloinnin kunnossa ja yhteysvalon näiden kahden laitteen välillä palamassa.

Konfigurointi tehtiin kytkimen konsoliportin kautta kannettavalla tietokoneella. Tähän prosessiin sisältyi IOS version tarkistus, aiemman konfiguraation tyhjennys, IP osoitteen määritys ja palvelimen pingaaminen (kuvio 26). IOS versio 12.1(22) EA2 ja myöhemmät versiot on todettu toimiviksi järjestelmän kanssa. On myös hyvä huomata, että ID 6 sai osoitteekseen 169.254.1.16 /24.

```
Switch> show ver

Switch> enable
Switch# write erase
Switch# reload

Switch# conf term

Switch(config)# snmp-server community netlab rw
Switch(config)# interface VLAN1
Switch(config-if)# ip address 169.254.1.11 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# exit

Switch# ping 169.254.1.1
```

Kuvio 26. Kytkimen konfiguraation komennot

Asennuksessa kaikki meni toivotulla tavalla ja laite sai yhteyden onnistuneesti palvelimeen. Lopuksi NETLAB+ konfiguroi kytkimen valmiiksi SNMP:lla ja testaa sen. Tämän seurauksena työssä saatiin kuvion 27 mukainen kontrollikytkin 6.

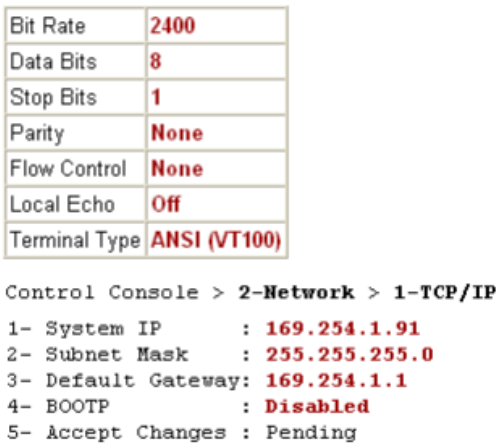


Kuvio 27. Kontrollikytkin ID 6

5.4.2 ACP PDU:n lisääminen järjestelmään

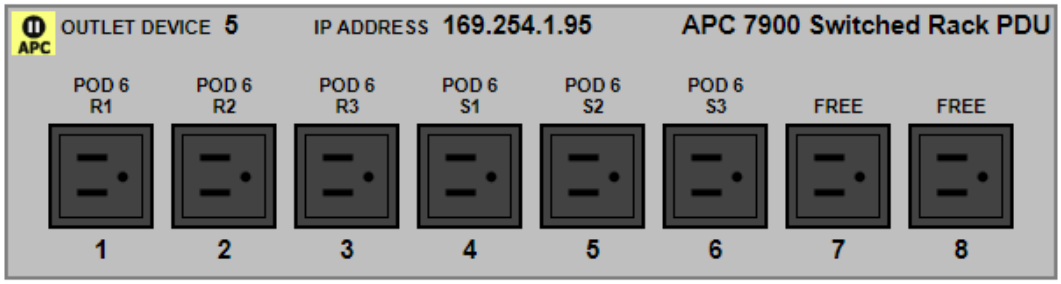
Virtalaitteen lisääminen noudattaa samaa kaavaa kuin kontrollikytkimen. Tämäkin toimenpide lähtee Control Devices -kuvakkeen alta, mutta etenee Switched Outlets -vaihtoehtoon. Add Switched Outled Device -valinta avaa täälläkin ikkunan, jossa määritellään uuden laitteen ID ja tyyppi.

PDU-laitteiden kohdalla tästä jatketaan kuitenkin suoraan konfigurointiin. Tämä suoritettiin ohjeiden suositusten takia kannettavalta tietokoneelta Hyperterm-sovelluksella. Kuviossa 28 näkyy sovelluksen asetukset ja esimerkki laitekonfiguraatiosta. Itse työssä lisätyt laitteet saivat .95, .96 ja .97 päätteiset osoitteen, niiden ID:n mukaan.



Kuvio 28. ACP PDU:n esimerkki konfiguraatio

Lopuksi tehdään yhteyden testaus pingaamalla, minkä jälkeen järjestelmä taas vie asennuksen loppuun ja testaa laitteen. Opinnäytetyössä tämä johti kolmeen kuvion 29 mukaiseen laitteeseen.



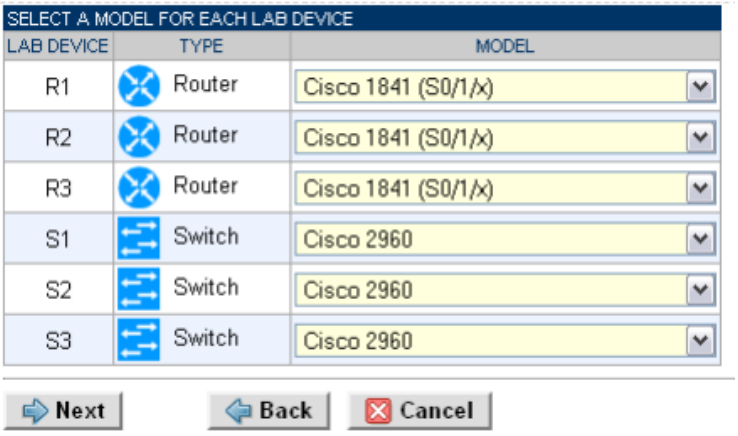
Kuvio 29. Outlet Device 5

5.4.3 Laitesolun lisääminen järjestelmään

Monikäyttöisen laitesolun lisääminen tapahtuu verkkokäyttöliittymän Equipment Pods -kuvakkeen takana. Add a Pod -painike johtaa listaan, mistä valitaan haluttu laitesolu.

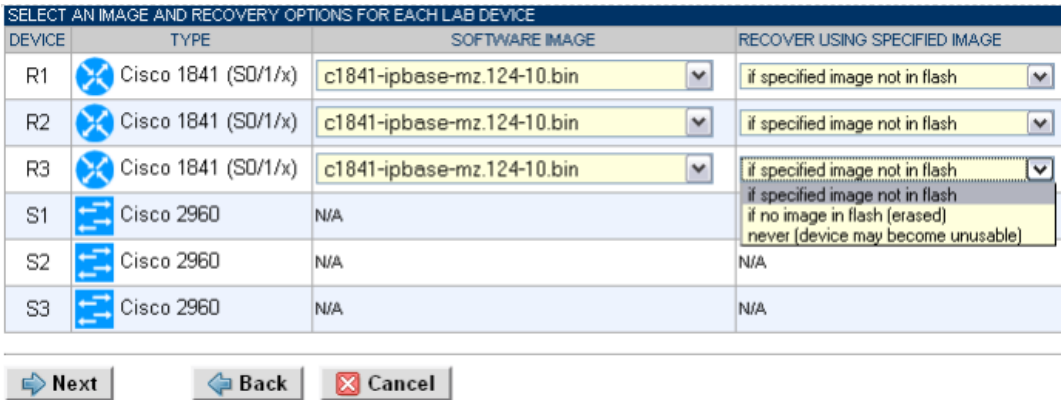
Kolme seuraavaa asennuksen askelta käsittävät resurssien varaamisen kontrollikytkimestä, yhteyspalvelimesta ja virtalaitteesta. On hyvä ottaa huomioon, että kontrollikytkimen porttien täytyy olla kahdeksan peräkkäistä, jotta asennus onnistuu (liite 2).

Yhteyspalvelimen (liite 3) ja virtalaitteiden suhteen ei ole samanlaista rajoitetta. Kyseisessä asennuksessa käytettiin kuitenkin samaa ratkaisua kaikkien varausten kohdalla, jotta johdonmukaisuus säilyi.



Kuvio 30. Mallin määrittäminen

Tämän jälkeen järjestelmälle pitää ilmoittaa, mitä mallia käytetyt laitteet ovat, kuten kuvissa 30. Kun malli on asetettu, jatketaan valitsemaan IOS image ja sen palautustapa (kuvio 31). Kyseessä on erittäin olennainen toiminto, koska IOS saatetaan poistaa laitteen muistista harjoitusten aikana.



Kuvio 31. IOS image

Seuraavaksi määritellään laitesolun ID ja nimi, minkä jälkeen solu lisätty NETLAB+ järjestelmään. Tavanomaisesti seuraava askel on itse kaapelointi. Opinnäytetyön laajennuksessa tämä osio oli jo suoritettu valmiiksi, mistä edettiin komponenttien konfigurointiin ja tarkistukseen.

```
switchport mode access
switchport nonegotiate
spanning-tree bpdufilter enable
no cdp enable
no keepalive
```

Control Switch ports

```
Lab Sw# configure terminal
Lab Sw(config)# boot enable-break
Lab Sw(config)# no boot system
Lab_Sw(config)# end
Lab_Sw# copy run start
```

Lab switches

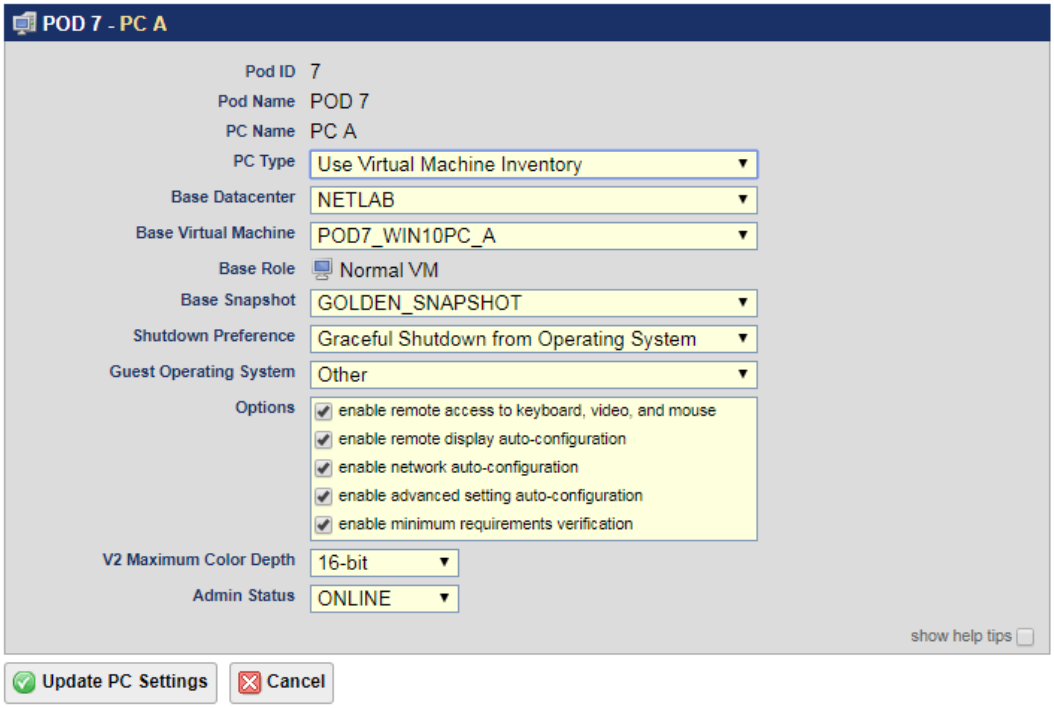
Kuvio 32. Kytkinten komennot

Konfigurointi käsittää kuviossa 32 näkyvät komennot. Ensimmäiset kontrollikytkimen käskyt sijoitetaan niihin portteihin, jotka ovat yhteydessä laitesolun omiin kytkimiin. Näin vältytään tietoliikenteen silmukoilta. Solun kytkimille puolestaan annetaan myöhemmät komennot, jotta järjestelmän on mahdollista hallinnoida laitteita halutulla tavalla.

Nyt vuorossa on laitesolun ensimmäinen testaaminen. Tällöin valitaan käyttöliittymästä testausvaihtoehto, minkä jälkeen järjestelmä ajaa omatoimisesti testin läpi. Ensimmäisessä työn testauksessa törmättiin muutamaan erilaiseen ongelmaan.

Ensimmäinen havaittu virhe oli yhdestä kytkimestä unohtuneet komennot (kuvio 32). Tämä kuitenkin nopeasti korjattu, minkä jälkeen laitesolu 6 läpäisi testauksen. Toinen ongelma ilmeni laitesolun 7 kanssa. Tuolloin yhdessä sen reitittimistä oli liian paljon dataa IOS asennusta varten. Ratkaisu oli ottaa konsoliyhteys laitteeseen ja tehdä manuaalisesti tilaa, minkä jälkeen tämäkin testi saatiin uudella yrityksellä läpi.

Toiseksi viimeinen vaihe asennuksessa on virtuaalikoneiden lisääminen. Tämä tapahtuu laitesolun virtuaalikoneikonien alla, missä niiden asetukset määritellään. Tästä esimerkkinä on kuviossa 33 laitesolun 7 valmiiksi konfiguroitu PC A. Tämä kyseinen tietokone luotiin ensin virtuaalikoneinventaarioon, mistä se yhdistettiin laitesolun osaksi.



Kuvio 33. Laitesolun 7 virtuaalikone PC A

Lopuksi ajetaan viimeinen testi laitesolun käyttöliittymän kautta. Mikäli kaikki menee toivotulla tavalla, testistä tulos on kuvion 34 mukainen, minkä jälkeen laitesolu voidaan ottaa käyttöön (kuvio 35). Työssä laitesolulla suoritettiin myös yksi harjoitustehtävä, jotta sen toimiminen voitiin todistaa henkilökohtaisesti.

ELAPSED	COMPLETED	PASSED	FAILED	SKIPPED	ERRORS	WARNINGS
00:08:12	37 of 37	37	0	0	0	0

Back To Pod Test Page

Kuvio 34. Läpäisty testi

POD 7 - STATUS

POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
7	POD 7	ONLINE	IDLE	MULTI-PURPOSE ACADEMY POD 3 Routers, 3 Switches

POD 7 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS LINES	SWITCHED OUTLETS	SOFTWARE IMAGE
	R1	Cisco 2801/2811 (S0/1/x)	AS 1 LINE 39 (tty 0/2/4)	SOD 6 OUTLET 1	c2801-adventerprisek9_ivs-mz.151-4.M10.bin
	R2	Cisco 2801/2811 (S0/1/x)	AS 1 LINE 40 (tty 0/2/5)	SOD 6 OUTLET 2	c2801-adventerprisek9_ivs-mz.151-4.M10.bin
	R3	Cisco 2801/2811 (S0/1/x)	AS 1 LINE 41 (tty 0/2/6)	SOD 6 OUTLET 3	c2801-adventerprisek9_ivs-mz.151-4.M10.bin
	S1	Cisco 2960	AS 1 LINE 42 (tty 0/2/7)	SOD 6 OUTLET 4	n/a
	S2	Cisco 2960	AS 1 LINE 43 (tty 0/2/8)	SOD 6 OUTLET 5	n/a
	S3	Cisco 2960	AS 1 LINE 44 (tty 0/2/9)	SOD 6 OUTLET 6	n/a

POD 7 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE / VM	OPERATING SYSTEM
	PC A	4309	ONLINE	POD7_WIN10PC_A	Other
	PC B	4310	ONLINE	POD7_WIN10PC_B	Other
	PC C	4311	ONLINE	POD7_WIN10PC_C	Other

POD 7 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
6	9-16	160	160-167

Pod 7 -- Management Options

Offline	Take this pod OFFLINE.
Test	Tell me if this pod is working properly.
Cable	Show me how to cable this pod.
Rename	Rename this pod.
Options	View and change special options for this pod.
Delete	Remove this pod from NETLAB.

Kuvio 35. Valmis laitesolu

5.5 Laajennuksen tulokset

Laajennuksen valmistuttua, etäkäyttöjärjestelmään oli lisätty kolme testattua monikäyttöistä laitesolua. Laitesolujen toiminnan kannalta olennaisten hallintalaitteiden lisääminen laskettiin osaksi prosessia, mikä kattaa kontrollikytkimen ja kolme virtalaitetta.

Laitesolujen käyttöönoton jälkeen varmistui, että valittu vaihtoehto täytti LAMK:n verkkotekniikan laboratorion tarpeet. Lisätyt solut mahdollistivat useampien samanaikaisten harjoitusten suorittamisen, eikä ASA-harjoitusten puuttuminen ollut ongelma.

Jatkon kannalta ASA-laitesolujen lisääminen järjestelmään on kuitenkin todennäköistä. Työssä laajennettu etäkäyttöjärjestelmä on nyt standardi monikäyttöisten laitesolujen yläarajassa. Tämän myötä tulevat laajennukset täytyy suorittaa ASA-soluilla tai käyttää muotista poikkeavaa vaihtoehtoa.

6 YHTEENVETO

Opinnäytetyön tavoite oli Lahden ammattikorkeakoulun verkkotekniikan laboratorion laajennus, millä haluttiin tehostaa verkkoharjoitusten tekoa. Työn käytännön osuus oli kaksiosainen, joista ensimmäinen osa käsitti kahden laajennusvaihtoehdon vertailun. Toinen osa puolestaan käsitti valitun vaihtoehdon mukaisen asennuksen, joka sisälsi kolme kokonaista laitesolua.

Vertailun kannalta oli samalla hyöty ja haitta, että MAP- ja MAPASA-laitesolut olivat erittäin samankaltaiset. Tämä nopeutti toimitusta mutta informaatiota oli myös vähemmän itse päätöstä varten. Lopulta vastakkain päätyivät MAP:n suoraviivaisempi toteutus ja MAPASA:n laajempi harjoitusvalikoima.

Fyysinen asennus eteni suuren osan ajasta ongelmitta, mihin osasyy oli LAMK:n aikaisempi kokemus järjestelmän kanssa. Tämä helpotti erityisesti laitteiden sijoittamisessa ja kaapeloinnissa, johon oli selkeä suunnitelma alusta loppuun asti. Toinen merkittävä tekijä oli NDG:n laadukas dokumentaatio laajennuksen teosta. Ohjeet olivat selkeät, kattavat ja hyvin toteutetut.

Laitteiden konfigurointi ja lisääminen järjestelmään saatiin suoritettua aikataulussa, muutamasta hidasteesta huolimatta. Järjestelmä varmisti vasta testauksessa, että kaikki vaaditut komennot oli annettu, minkä takia ensimmäistä laitesolua tuli konfiguroitua kahteen kertaan. Tältä vältyttiin toisen ja kolmannen solun kohdalla manuaalisella tarkistuksella.

Osaan asennuksessa käytetyistä reitittimistä oli myös jäänyt tiedostoja, jotka estivät järjestelmää siirtämästä IOS imageja niihin. Ongelma korjattiin tekemällä laitteisiin tilaa manuaalisesti, mutta siltä olisi voitu välttyä jo valmistelun aikana. Tämän korjauksen aikana myös yksi laitteista jäi kokonaan ilman IOS imagea, mikä ratkaistiin järjestelmän palautustyökalun avulla.

Käyttöönoton jälkeen paljastui, että valittu MAP-laajennus riitti kattamaan työn tavoitteet, mutta MAPASA laajennus voi silti tulla ajankohtaiseksi. Tämä johtuu siitä, että asennus saavutti käytössä olevan järjestelmän MAP-laitesolujen ylärajan. Jatkossa järjestelmää voidaan laajentaa MAPASA:n voimin tai muutamalla uniikilla laitesolulla, ellei itse versiota vaihdeta.

Etäkäytön suosio on ollut kasvussa jo tovin, eikä tämä suuntaus näytä muuttumisen merkkejä. Tekniikan sovelluksia kehitetään jatkuvasti ja ne on suunnattu niin yritysten kuin myös yksityishenkilöiden käyttöön. Etätyön yleistymisen myötä tällaiset ratkaisut ovat jo

osa arkea. Näiden havaintojen pohjalta etäkäytön tulevaisuus näyttää lupaavalta, sillä teknologia ei ole vielä saavuttanut lakipistettään.

LÄHTEET

Allied Telesis 2015. SNMP Feature Overview Guide [viitattu 28.3.2018]. Saatavissa: https://www.alliedtelesis.com/sites/default/files/snmp_feature_overview_guide.pdf

Bretz, R. 2006. Das Prinzip der SNMP-Kommunikation [viitattu 28.3.2018]. Saatavissa: https://commons.wikimedia.org/wiki/File:Snmp.PNG

Burnett, C.M.L. 2008. Encapsulation of application data descending through the layered IP architecture [viitattu 21.3.2018]. Saatavissa: https://commons.wikimedia.org/wiki/File:UDP_encapsulation.svg

Cisco Press 2002. VPNs and VPN Technologies [viitattu 7.3.2018]. Saatavissa: http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=7

COLMAN IT 2017. Remote Access [viitattu 24.2.2018]. Saatavissa: http://www.colmanit.com.au/remote-access/

Egli, P.R. 2015. Trivial File Transfer Protocol [viitattu 28.3.2018]. Saatavissa: http://www.indigoo.com/dox/itdp/07_FTP-TFTP/TFTP.pdf

Frankel, S. 2001. Demystifying the IPsec Puzzle. Artech House.

Geerling, J. 2014. A brief history of SSH and remote access [viitattu 24.2.2018]. Saatavissa: https://www.jeffgeerling.com/blog/brief-history-ssh-and-remote-access

Koivunen, E. 2010. Verkon aktiivilaitteet [viitattu 26.3.2018]. Saatavissa: https://www.vahtiohje.fi/web/guest/verkon-aktiivilaitteet

Koulutus- ja konsultointipalvelu KK Mediat 2018. VPN-verkot [viitattu 3.3.2018]. Saatavissa: http://www.2kmediat.com/vpn/yhteys.asp

Kozierok, C.M. 2005. TFTP Write Process [viitattu 29.3.2018]. Saatavissa: http://www.tcpipguide.com/free/t_TFTPDetailedOperationandMessaging-3.htm

McCabe, J.D. 2007. Network Analysis, Architecture, and Design. Morgan Kaufmann cop. 3rd edition.

LAMK 2018. Organisaatio [viitattu 24.2.2018]. Saatavissa: http://www.lamk.fi/lamk-oy/organisaatio/Sivut/default.aspx

Microsoft. 2018. Remote Access [viitattu 24.2.2018]. Saatavissa: https://msdn.microsoft.com/en-us/library/windows/desktop/bb545687(v=vs.85).aspx

Miller, P. & Cummins, M. 2000. Lan Technologies Explained. Butterworth-Heinemann. Digital Press

NDG 2009. NDG NETLAB+ System Overview [viitattu 9.3.2018]. Saatavissa: https://www.netdevgroup.com/support/documentation/netlab_system_overview.pdf

NDG 2015. INSTALLATION AND CONFIGURATION GUIDE Multi-Purpose Academy Pod [viitattu 1.4.2018]. Saatavissa: https://www.netdevgroup.com/content/cnap/documentation/netlab_multipurpose_academy_pod.pdf

NDG 2018. INSTALLATION AND CONFIGURATION GUIDE Multi-Purpose Academy Pod with ASA [viitattu 1.4.2018]. Saatavissa: https://www.netdevgroup.com/content/cnap/documentation/netlab_multipurpose_academy_pod_asa.pdf

NETGEAR 2005. Virtual Private Networking Basics [viitattu 3.3.2018]. Saatavissa: http://documentation.netgear.com/reference/enu/vpn/pdfs/FullManual.pdf

Oppliger, R. 2016. SSL and TLS Theory and Practice. Artech House Publishers.

Palo Alto Networks 2018a. What is a vpn? [viitattu 3.3.2018]. Saatavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn

Palo Alto Networks 2018b. What is remote access? [viitattu 24.2.2018]. Saatavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-remote-access

Puska, M. 2000. Lähiverkkojen tekniikka pro training. Satku – Kauppakaari. Jyväskylä: Gummerus Kirjapaino Oy

Techopedia 2018a. Remote Access [viitattu 24.2.2018]. Saatavissa: https://www.techopedia.com/definition/5553/remote-access

Techopedia 2018b. Network Protocols [viitattu 24.2.2018]. Saatavissa: https://www.techopedia.com/definition/12938/network-protocols

White, C.M. 2011. Fundamentals of Networking and Data Communications, Sixth Edition. Cengage Learning.

Wikipedia 2018a. Network switch [viitattu 2.4.2018]. Saatavissa: https://en.wikipedia.org/wiki/Network_switch

Wikipedia 2018b. Router (computing) [viitattu 2.4.2018]. Saatavissa: https://en.wikipedia.org/wiki/Router_(computing)

Wikipedia 2018c. Simple Network Management Protocol [viitattu 29.3.2018]. Saatavissa: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

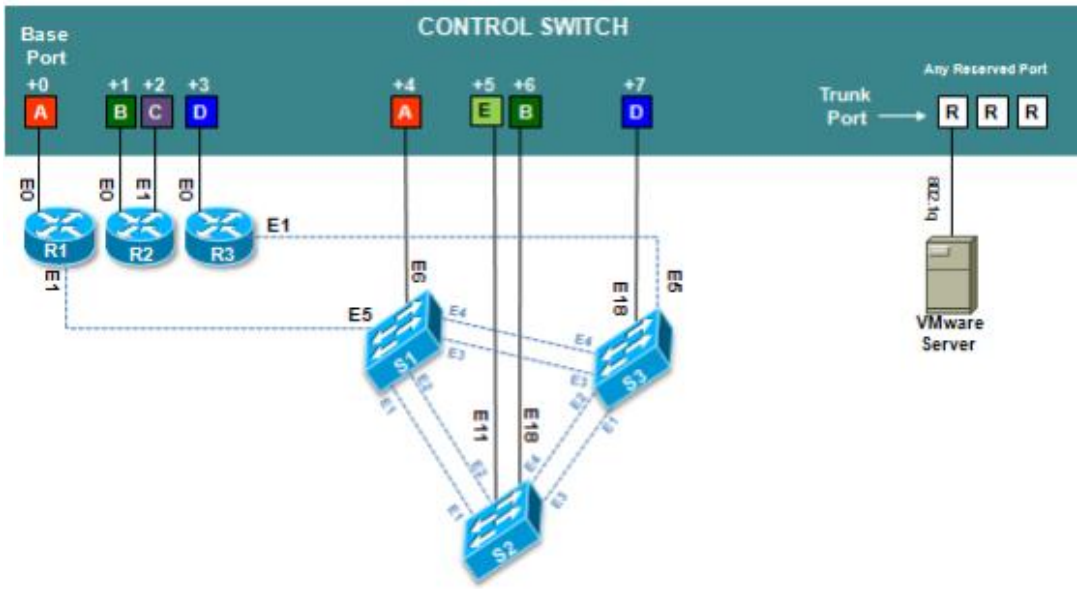
Wikipedia 2018d. TCP/IP-viitemalli [viitattu 23.3.2018]. Saatavissa: https://fi.wikipedia.org/wiki/TCP/IP-viitemalli

Wikipedia 2018e. Virtual private network [viitattu 28.3.2018]. Saatavissa: https://en.wikipedia.org/wiki/Virtual_private_network

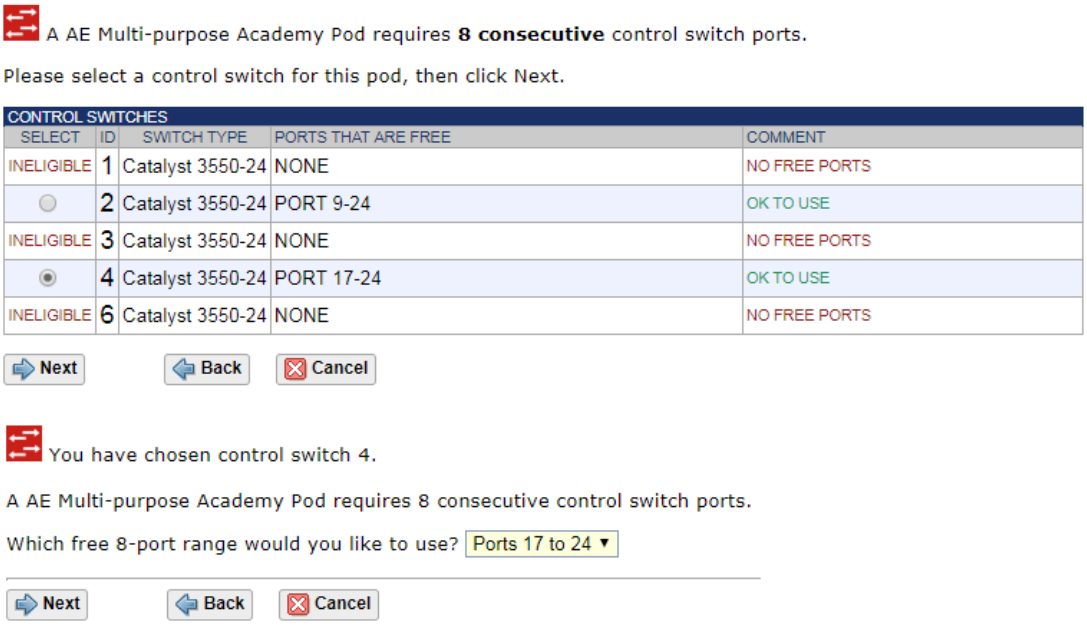
Wilkins, S. 2012a. OSI Model [viitattu 23.3.2018]. Saatavissa: http://www.pearsonitcertification.com/articles/article.aspx?p=1829351

Wilkins, S. 2012b. TCP/IP Model [viitattu 23.3.2018]. Saatavissa: http://www.pearsonitcertification.com/articles/article.aspx?p=1829351

LIITTEET



Liite 1. MAP:n liitos kontrollikytkimeen (NDG 2015, 13)



A AE Multi-purpose Academy Pod requires **8 consecutive** control switch ports.

Please select a control switch for this pod, then click Next.

CONTROL SWITCHES

SELECT	ID	SWITCH TYPE	PORTS THAT ARE FREE	COMMENT
INELIGIBLE	1	Catalyst 3550-24	NONE	NO FREE PORTS
○	2	Catalyst 3550-24	PORT 9-24	OK TO USE
INELIGIBLE	3	Catalyst 3550-24	NONE	NO FREE PORTS
◉	4	Catalyst 3550-24	PORT 17-24	OK TO USE
INELIGIBLE	6	Catalyst 3550-24	NONE	NO FREE PORTS

Next Back Cancel

You have chosen control switch 4.

A AE Multi-purpose Academy Pod requires 8 consecutive control switch ports.

Which free 8-port range would you like to use? Ports 17 to 24 ▾

Next Back Cancel

Liite 2. Kontrollikytkimen porttien määritys

A AE Multi-purpose Academy Pod requires **6** access server lines.

It is a good idea to use consecutive lines on one access server if possible. This practice will make it easier to cable and troubleshoot. If consecutive lines are not available, you can use non-consecutive lines, spanning multiple access servers if necessary.

ACCESS SERVERS

ID	TYPE	LINES THAT ARE FREE
1	Cisco 2901 + 4 HWIC-16A (Lines 3-66)	51-66

A AE Multi-purpose Academy Pod requires **6** access server lines.

◉ Use 6 consecutive lines on access server 1 ▾ starting at Line 3 | HWIC-16A 0/0/0 | CAB-HD8-ASYNC P0 ▾
○ Let me pick the access server and lines for each device

Liite 3. Yhteyspalvelimen linjojen määritys

Control Switches

COMPLETED 2 of 2
PASSED 2

PING Ping pod's control switch (control switch 6, 169.254.1.16). LOG PASSED
5 pings, 5 replies, min/avg/max = 0.6/0.6/0.6 (ms)

SETUP Setup control switches. LOG PASSED
Pod 7 using control switch VLAN 160 through 167.
Pod 7 using port(s) 9 through 16 on control switch 6.

Liite 4. Testin läpäissyt kontrollikytkin

R1

COMPLETED 5 of 5
PASSED 5

CONSOLE Power up and receive console output. LOG PASSED
c2801 platform with 393216 Kbytes of main memory
System Bootstrap, Version 12.4(13r)T5, RELEASE SOFTWARE (fc1)
Device is powered on and receiving console output.

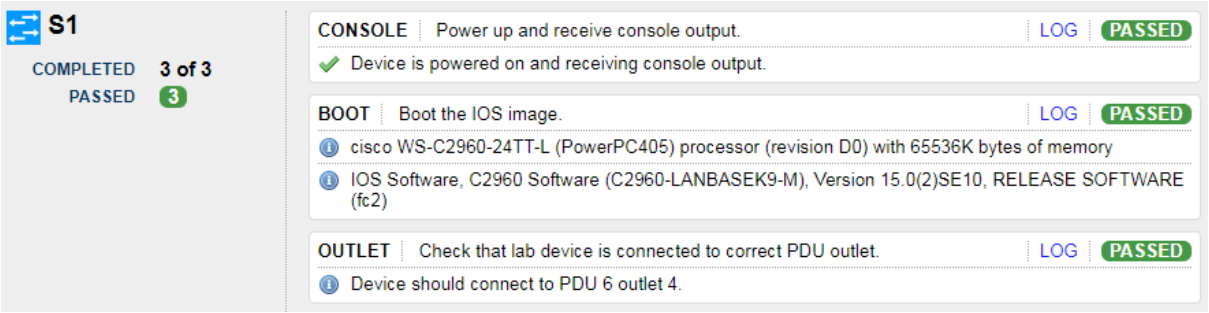
BOOT Boot the IOS image. LOG PASSED
Cisco IOS Software, 2801 Software (C2801-ADVENTERPRISEK9_IVS-M), Version 15.1(4)M10, RELEASE SOFTWARE (fc2)

FLASH Check image and size of flash memory. LOG PASSED
Image 'c2801-adventerprisek9_ivs-mz.151-4.M10.bin' (60271616 bytes) will fit in flash (128733184 bytes).

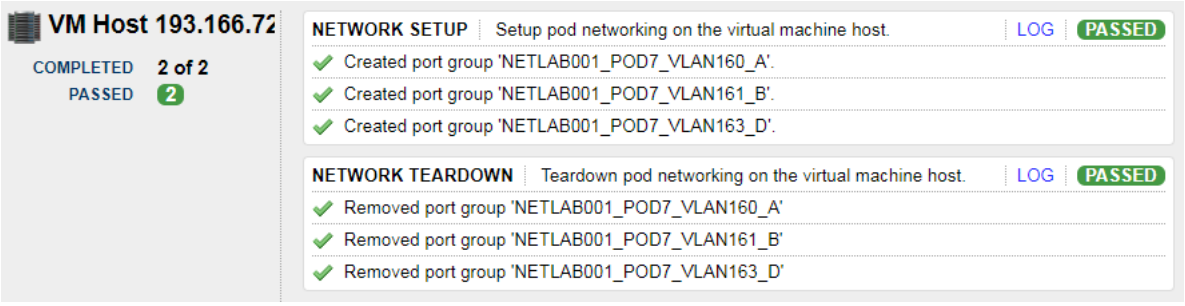
NETWORK Check proper ethernet cabling between lab device and control switch. LOG PASSED
Device interface FastEthernet0/0 should connect to control switch 6 port 9.
The NETLAB+ inside server interface was pinged via FastEthernet0/0.

OUTLET Check that lab device is connected to correct PDU outlet. LOG PASSED
Device should connect to PDU 6 outlet 1.

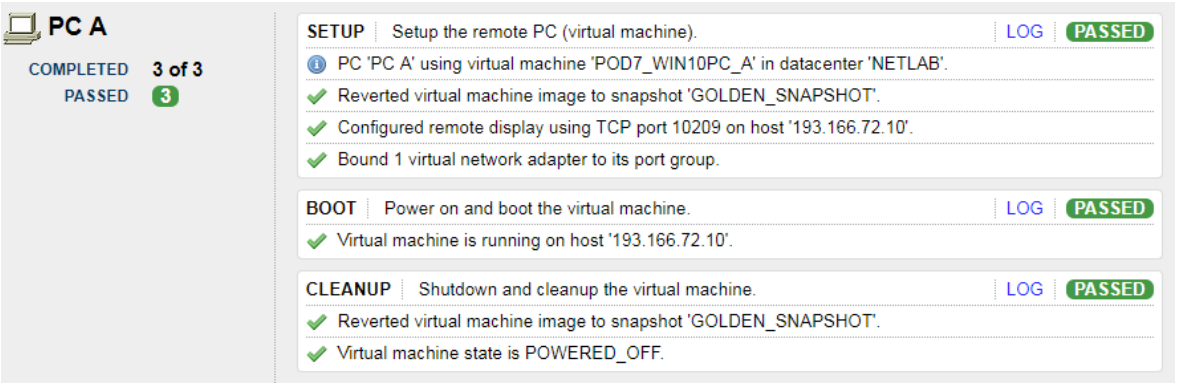
Liite 5. Testin läpäissyt reititin



Liite 6. Testin läpäissyt kytkin



Liite 7. Testin läpäissyt VM HOST



Liite 8. Testin läpäissyt virtuaalikone